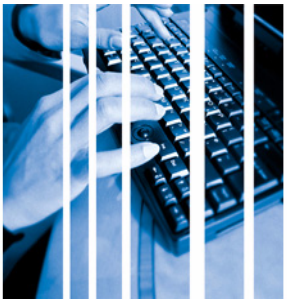
[SafeGuard® Easy]

[Zugangsschutz durch Verschlüsselung]



Version 4.50.3

Windows® Server 2003
Windows® XP
Windows® 2000

utimaco®
safeware

Alle Rechte vorbehalten.

Kein Teil dieser Dokumentation darf in irgendeiner Form (Druck, Fotokopie oder einem anderen Verfahren) ohne schriftliche Genehmigung der Utimaco Safeware AG für andere Zwecke als den Eigengebrauch reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

Die Utimaco Safeware AG behält sich das Recht vor, die Dokumentation ohne vorherige Ankündigung jederzeit zu ändern oder zu ergänzen. Für Druckfehler und dadurch entstandene Schäden übernimmt die Utimaco Safeware AG keine Haftung.

CryptoServer und SafeGuard sind eingetragene Marken der Utimaco Safeware AG.

Windows, Windows 2000, Windows XP und Windows Server 2003 sind eingetragene Marken der Microsoft Corporation.

Patents rights of Ascom Tech Ltd. given in EP, JP, US. IDEA is a Trademark of Ascom, Tech Ltd.

Andere in diesem Handbuch erwähnte Marken- und Produktnamen sind Marken der jeweiligen Rechtsinhaber und werden hiermit anerkannt.

Microsoft, Windows, und das Windows Logo sind Marken der Microsoft Corporation in den Vereinigten Staaten und/oder anderen Ländern.

Utimaco Safeware AG
Postfach 20 26
61410 Oberursel
Tel (06171) 88-0
Fax (06171) 88-10 10
info.pds@utimaco.com
http://www.utimaco.com

© Utimaco Safeware AG 2008

Technischer Support

Online Dokumentation

Unsere Wissensdatenbank bietet Antworten auf viele typische Fragen rund um die SafeGuard Produktpalette, so zum Beispiel zu Funktionsumfang, Implementierung, Administration oder Troubleshooting.

Direkter Link: http://www.utimaco.de/myutimaco

Für den Zugang zum öffentlichen Bereich der Wissensdatenbank können Sie sich als Gast anmelden. Für den Zugang zum geschützten Bereich benötigen Sie einen gültigen Softwarepflegevertrag. Der Inhalt beider Bereiche wird von unseren Support Mitarbeitern fortwährend überarbeitet und auf aktuellem Stand gehalten.

Weitergehender Support bzw. Telefon Support

Kunden mit einem gültigen Softwarepflegevertrag inklusive Servicevereinbarung stehen qualifizierte Support-Mitarbeiter auch telefonisch mit Rat und Tat zur Seite.

Für ein individuelles Vertragsangebot wenden Sie sich an Ihren Utimaco Vertriebspartner.

Wir bitten um Ihr Verständnis, dass Anfragen von Kunden ohne gültigen Softwarepflegevertrag / Software Subscription je nach Aufkommen einige Arbeitstage in Anspruch nehmen können. In dringenden Fällen wenden Sie sich bitte an den Utimaco Vertriebspartner, über den Sie Ihre Lizenzen bzw. Software Subscription bezogen haben.

1 Überblick 1

1.1 Zentrale Sicherheitsfunktionen 2

1.2 Weitere Sicherheitsfunktionen 4

1.3 Neues in SafeGuard Easy 11

1.4 Änderungen zu Vorgängerversionen 13

1.5 Systemvoraussetzungen 14

1.6 Dokumentation 17

1.7 Allgemeine Hinweise 17

1.8 Lizenzhinweise 18

2 Erste Schritte 19

2.1 Installation vorbereiten 19

2.2 Installationsvoraussetzungen 21

2.3 Installierbare Module 22

2.4 Sprache der Benutzeroberfläche 23

3 Lokale Installation 25

3.1 Schritt-für-Schritt-Anleitung 26
3.1.1 Verschlüsselungsmodus 31

3.2 Nach der Installation 33

3.3 Verschlüsselungsfortschritt 35
3.3.1 Verschlüsselungsfortschritt ausschalten 35
3.3.2 Verschlüsselungsgeschwindigkeit definieren 36

3.4 Hintergrund-Bitmap in der Windows-Anmeldung austauschen 39

3.5 SafeGuard Easy auf einem PC mit mehreren Betriebssystemen installieren 41

4 Zentrale Installation 43

4.1 Konfigurationsdatei erstellen 44

4.2 Zentrale Installation mit Active Directory..... 45
4.2.1 Voraussetzungen 45
4.2.2 MSI-Pakete mit einem Editor bearbeiten 46

4.3 Zentrale Installation ohne Active Directory 49
4.3.1 Kommandozeile für automatische Installation. 49
4.3.2 Ausgewählte Optionen des Windows-Installers 51

4.4 SafeGuard Easy Funktionen und Parameter 52
4.4.1 SafeGuard Easy Funktionen 52
4.4.2 SafeGuard Easy Parameter 56

5 Update..... 59

5.1 Lokales Update 60

5.2 Update mit Migrationsdatei 65

5.3 Systemkern-Prüfung beim Update..... 67
5.3.1 Was passiert, wenn der Systemkern nicht in Ordnung ist..... 67
5.3.2 Über das Reparaturprogramm..... 68
5.3.3 Parameter für das Reparaturprogramm 69

6 Deinstallation 71

6.1 Lokale Deinstallation 72

6.2 Deinstallation mit Challenge/Response 73

6.3 Vorkonfigurierte Deinstallation mit Konfigurationsdatei 75

7 Systemstart und Anmeldung 77

7.1 Als regulärer Benutzer anmelden 78

7.2 Als Standardbenutzer anmelden 79

7.2.1 Erweiterte Anmeldung über die Taste [F2] 79

7.3 Mit Token anmelden 80

7.4 SafeGuard Easy-Passwort über die Taste [F10] ändern 81

7.5 Vergessene Passwörter über die Taste [F9] zurücksetzen 82

7.6 Fehlgeschlagene Anmeldung 83

7.7 Anmeldung mit Pre-Boot Authentisierung über die Taste [F2] erzwingen 84

7.8 Automatische Anmeldung an das Betriebssystem 85

7.9 Kompatibilität mit Anmeldekomponenten anderer Hersteller 86

8 Verwaltung im Überblick 89

8.1 Funktionstrennung 89

8.2 Administration und Konfigurationsdatei-assistenten starten 91

8.3 Die Administration 92
8.3.1 Administrations-Fenster 93
8.3.2 Symbol- und Werkzeugleiste 95

8.4 Konfigurationsdateiassistent 96
8.4.1 Konfigurationsdateien aus älteren SafeGuard Easy-Versionen wiederverwenden. 97
8.4.2 Neue Konfigurationsdatei erstellen 98
8.4.3 Konfigurationsdatei für Installation erstellen .. 99
8.4.4 Konfigurationsdatei zur Deinstallation erstellen 103
8.4.5 Konfigurationsdatei für Änderung („Delta-Datei“) erstellen 104
8.4.6 Delta-Datei ausführen 108
8.4.7 Konfigurationsdatei editieren 109
8.4.8 Anwendungsbeispiele 109

8.5 Konfigurationsdatei über Kommandozeile erzeugen 112

8.6 Häufig verwendete Registry-Einstellungen für SafeGuard Easy über die administrative Vorlage ändern 114

9 Pre-Boot Authentisierung 117

9.1 Sprache der Pre-Boot Authentisierung nachträglich ändern 118

9.2 Passwort beim Systemstart abfragen 119

9.3 Identifikation 120

9.3.1 Maschinen Identifikation 120
9.3.2 Begrüßungstext 122

10 Master Boot Record 123

10.1 MBR-Schutz 125

10.2 MBR (Standard) Aktionen 126

10.3 Unterstützung für Compaq Setup-Partition 127

11 Verschlüsselung 129

11.1 Verschlüsselung konfigurieren 131

11.2 Unterstützte Festplattenlaufwerke 132

11.3 Unterstützte Diskettenlaufwerke 134

11.4 Unterstützte Wechselmedienlaufwerke 134

11.5 Laufwerke verschlüsseln 135

11.6 Schlüssel 137
11.6.1 Schlüsselmanagement 137
11.6.2 Schlüsselerzeugung 138
11.6.3 Schlüssellänge 138
11.6.4 Triviale Schlüssel 139
11.6.5 Zufallsschlüssel 139
11.6.6 Schlüssel definieren 139
11.6.7 Schlüssel ändern 140

11.7 Algorithmen 141
11.7.1 Algorithmus wählen 141
11.7.2 SafeGuard Easy Algorithmen 141
11.7.3 Algorithmus ändern 144

11.8 Verschlüsselungsstatus im Windows-Explorer anzeigen 145

11.9 Image einer verschlüsselten Festplatte erstellen 146

12 Benutzerprofile erstellen 149

12.1 Festlegen von Verwaltungsaufgaben 150

12.2 Vordefinierte Benutzer 151
12.2.1 Der Benutzer SYSTEM 151
12.2.2 Der Benutzer USER 151
12.2.3 Der *AUTOUSER 152

12.3 Benutzer anlegen 153

12.4 Benutzer kopieren 154

12.5 Benutzer löschen 155

12.6 Benutzermerkmale 156
12.6.1 Benutzernamenmindestlänge 156
12.6.2 Token-Anmeldung 156
12.6.3 Standardbenutzer 157
12.6.4 Verkürzten C/R Code erzeugen 157
12.6.5 Schablone 157
12.6.6 Ablaufdatum 159

12.7 Benutzerrechte 160
12.7.1 Benutzerrechte zuweisen 162
12.7.2 Benutzerrechte weitergeben 163

13 Passworteinstellungen 165

13.1 Vordefinierte Passwortregeln 166

13.2 Erlaubte Tasten für das SafeGuard Easy-Passwort 167

13.3 SafeGuard Easy für Einsatz im internationalen Umfeld konfigurieren 168

13.3.1 Effekte verschiedener Tastaturlayouts 168
13.3.2 International einheitliche Zugangsdaten für SafeGuard Easy erzeugen 169

13.4 Allgemeine Passwortregeln 171
13.4.1 Passworteingabe beim Systemstart abfragen 172
13.4.2 Passworteingabe verdecken 172
13.4.3 Mindestlänge der Passwörter 172
13.4.4 Mindestalter der Passwörter 172
13.4.5 Passwortgenerationen 173
13.4.6 Mindestanzahl an Buchstaben, Zahlen, Symbolen 174
13.4.7 Groß-/Kleinschreibung verwenden 174

13.5 Verbotene Passworte 175
13.5.1 Verbotene Passworte definieren 175
13.5.2 Passwortliste importieren 176

13.6 Benutzerspezifische Passwortregeln 177
13.6.1 Passwortwechsel erlauben 177
13.6.2 Passwortwechsel nach (´n´ Tagen) 178
13.6.3 Passwortänderung bei nächster Anmeldung. 178

13.7 Passwort definieren 179

14 Twinboot/Bootmanager 181

14.1 Funktionsweise 181

14.2 Voraussetzungen 182

14.3 Beispiel 183

14.4 Twinboot konfigurieren 184

14.5 Bootmanager konfigurieren 186
14.5.1 Allgemeine Einstellungen 186
14.5.2 Startlaufwerke 187

14.6 Daten zwischen Bootpartitionen austauschen .. 190

15 Token-Unterstützung 191

15.1 Vorteile einer Anmeldung mit Token 192

15.2 Unterstützte Token 194

15.3 Token-Funktionen 195

15.4 Token-Unterstützung installieren 196

15.5 Das erste Mal mit Token in der Pre-Boot Authentisierung anmelden 199

15.6 Token-Passwort ändern 201

15.7 SafeGuard Easy-Zugangsdaten auf dem Token ändern/löschen 201

15.8 Token ausstellen 202
15.8.1 Token-Ausstellungsmodus 202
15.8.2 Token-Ausstellung automatisieren 204

15.9 Mit Token an den Administrationswerkzeugen anmelden 209
15.9.1 Token-Unterstützung für die Administrationswerkzeuge installieren 210
15.9.2 PKCS#11 Modul des Token registrieren 211
15.9.3 Universal Token Interface 213

15.10 Anmeldung mit Token an das Betriebssystem 216
15.10.1 Betriebssystemdaten auf den Token schreiben 217
15.10.2 Gespeicherte Windows-Daten in der SAL-Datei 218

15.11 Token mit der Token Administration zentral ausstellen 219
15.11.1 Token Administration installieren 220
15.11.2 SafeGuard Easy-Zugangsdaten auf dem Token löschen 221

15.11.3 SafeGuard Easy-Zugangsdaten aus Konfigurationsdatei importieren 222

15.12 SafeGuard Easy-Benutzer schnell wechseln 224
15.12.1 Voraussetzungen 225
15.12.2 Beispiel 225

15.13 Hilfe im Notfall 227
15.13.1 Voraussetzungen 228
15.13.2 Einsatzbeispiele 229
15.13.3 Token remote verwalten 233

16 Mit Lenovo Fingerabdruck-Leser anmelden 235

16.1 Voraussetzungen 236

16.2 Unterstützte Hardware 237

16.3 Unterstützung für Lenovo Fingerabdruck installieren 239

16.4 SafeGuard Easy-Passwort ändern..... 242

16.5 Häufig gestellte Fragen 243

17 Windows-Anmeldung konfigurieren 245

17.1 Sicherer automatischer Logon (SAL) 246
17.1.1 Sicheren automatischen Logon (SAL) einschalten 247
17.1.2 Anmeldung an Windows mit Smartcard (Smartcard-SAL) 250
17.1.3 SAL/Smartcard-SAL ausschalten 252
17.1.4 SAL-Dialog unterdrücken 254
17.1.5 SAL/Smartcard-SAL Daten löschen 255
17.1.6 Restriktion..... 256

17.2 Identisches Passwort für Windows und SafeGuard Easy (Passwortsynchronisierung)..... 257

17.2.1 Vorteile der Passwortsynchronisierung 258
17.2.2 Passwortsynchronisierung vorbereiten 258
17.2.3 Passwortsynchronisierung einschalten..... 259
17.2.4 Passwortsynchronisierung durchführen 260
17.2.5 Windows-Kennwort ändern bei aktiver Passwortsynchronisierung..... 263
17.2.6 SafeGuard Easy-Passwort wechseln 264
17.2.7 Dialog zur Passwortsynchronisierung abbrechen 265
17.2.8 Einschränkungen..... 265
17.2.9 Was tun, wenn... 267

17.3 Zusätzliche Optionen für die Windows-Anmeldung..... 268
17.3.1 Windows An-/Abmeldung 269
17.3.2 Rechnersperre 273
17.3.3 Bildsschirmschoner 274
17.3.4 Authentisierungsmodul (GINA) reparieren.... 278
17.3.5 Novell Anmeldung..... 279

18 Arbeitsplatzsperre von SafeGuard Easy..... 281

18.1 Voraussetzungen 282

18.2 Windows-Bildschirmschoner mit Kennwortschutz aktivieren 283

18.3 SafeGuard Easy Arbeitsplatzsperre nicht anzeigen..... 285

19 Sicheres Wake On LAN 287

19.1 Überblick..... 287

19.2 Sperre der Windows-Anmeldung 288

19.3 Wake On LAN-Meldung anpassen 289

19.4 Wake On LAN Sperre temporär aufheben 290
19.5 Wake on LAN konfigurieren 291

20 Ruhezustand (Hibernation) 293

20.1 Überblick 293
20.2 Ruhezustand und SafeGuard Easy 294
20.3 Voraussetzungen und Restriktionen 295
20.4 Ruhezustand einrichten 296

21 Disketten- und Geräteverschlüsselung schalten 297

21.1 Notwendige SafeGuard Easy-Rechte 298
21.2 Verschlüsselung schalten 299
21.3 Schlüssel setzen mit SgeCrypt 300
21.3.1 Temporäre Schlüssel nicht zurücksetzen 301
21.4 Verschlüsselungseinstellungen über Kommandozeile schalten 303
21.5 Hinweise zur Disketten- und Geräteverschlüsselung 304

22 FIPS 140-2 (Level 1) Zertifizierung 305

22.1 Neue Funktionen für FIPS 306
22.2 SafeGuard Easy FIPS-konform installieren 307

22.3 Sicherer Einsatz von SafeGuard Easy in zertifizierter Konfiguration 309

23 SafeGuard Easy und Lenovo Thinkvantage Technologien - Embedded Security Subsystem (ESS Chip).. 311

23.1 SafeGuard Easy und TPM..... 313

23.2 Chip-Nutzung vorbereiten..... 314

23.3 Erforderliche Einstellungen für Client Security Integration 315

23.4 Erforderliche Einstellungen für die Erzeugung von Zufallsschlüsseln über den TPM Chip 318

23.5 Erforderliche Einstellungen für die Sicherung der Client-/Server-Authentisierung über den TPM Chip 319

23.6 Erforderliche Einstellungen für die Maschinenbindung..... 323
23.6.1 Initiale Maschinenbindung 324
23.6.2 Maschinenbindung gescheitert..... 326
23.6.3 Maschinenbindung Wiederherstellung..... 327
23.6.4 Konfiguration des Wiederherstellungsmodus 330

24 SafeGuard Easy und Lenovo Thinkvantage Technologien - Rescue and Recovery™ 333

24.1 Überblick..... 333

24.2 Rescue and Recovery und SafeGuard Easy..... 334

24.2.1 Vorteile der Kombination Rescue and Recovery und SafeGuard Easy... 335
24.2.2 Voraussetzungen 335

24.3 Installation 336
24.3.1 Weder SafeGuard Easy noch Rescue and Recovery™ sind installiert 337
24.3.2 Nur SafeGuard Easy ist bereits installiert..... 338

24.4 Upgrade 340
24.4.1 Upgrade von SafeGuard Easy..... 340
24.4.2 Upgrade von Rescue and Recovery 340

24.5 Deinstallation 340

24.6 Sicherungskopie erstellen..... 341

24.7 Dateien aus SafeGuard Easy-Backup wiederherstellen 343

24.8 SafeGuard Easy-System wiederherstellen 344
24.8.1 Boot-Umgebung..... 345
24.8.2 Vorgehensweise..... 345

24.9 Service Partition und Factory Recovery Partition 346
24.9.1 Besonderheiten 347

24.10 Was tun, wenn... 349

25 Kompatibilität zur Computrace Software der Absolute Software Corp..... 351

26 Fernwartung (Challenge/Response) 353

26.1 Funktionsweise 354
26.1.1 Response Code Assistenten für PDA installieren 355

26.2 Challenge Code erzeugen 356

26.3 Response Code 358
26.3.1 Response Code erzeugen 359

26.4 Erweiterung des Challenge/Response Konzepts 367
26.4.1 Helpdesk-Konsole 367
26.4.2 Web Self Help 368
26.4.3 VOICE.TRUST 369

27 Notfallmedien erstellen und Systemkern sichern 371

27.1 Notfalldiskette erstellen 372
27.1.1 Notfallassistenten starten 373
27.1.2 Systemkern per Kommandozeile sichern 376
27.1.3 SafeGuard Easy Notfalldateien manuell auf Diskette sichern 376

27.2 Bootfähige Notfalldiskette erstellen 377

27.3 Bootfähige Notfall-CD erstellen 378

27.4 Bootfähigen Notfall-USB-Stick erstellen 379

27.5 Notfallstart durchführen 380
27.5.1 Systemkern restaurieren 381
27.5.2 Systemkern reparieren 382
27.5.3 Notfalldeinstallation von SafeGuard Easy 383
27.5.4 Hinweise 385

27.6 Nach Booten von externen Medien im Notfall auf verschlüsselte Daten zugreifen 386
27.6.1 Voraussetzung 387
27.6.2 Vorgehensweise 388
27.6.3 Hinweise 389
27.6.4 Was tun, wenn... 390

28 Systemstatus von SafeGuard Easy anzeigen 391

28.1 Reporting 391

28.2 Parameter 392

29 Protokollierung 393

29.1 Anwendungsgebiete 394

29.2 Protokollierung installieren 395

29.3 Protokollierung konfigurieren 396

29.4 Ereignisse protokollieren 397
29.4.1 Ziel festlegen 397
29.4.2 Neues Ziel erzeugen 398
29.4.3 Ziel löschen 400
29.4.4 Ziel kopieren 400

29.5 Ereignisse auswählen 401
29.5.1 Alle Ereignisse konfigurieren 403
29.5.2 Ansicht ändern 404

29.6 Protokollierte Ereignisse ansehen 405
29.6.1 Ereignisanzeige (Event Log) 406
29.6.2 Protokolldatei (Log File) 408

29.7 Hinweise 409

30 Zentrale Administration 411

30.1 Funktionsweise 412
30.1.1 SafeGuard Easy Server/SafeGuard Easy Datenbank 414
30.1.2 SafeGuard Easy Administrationskonsole 416
30.1.3 SafeGuard Easy Clients 417

30.1.4 Unterstützte SafeGuard Easy Client-/ SafeGuard Easy Server-Kombinationen 418

30.2 Datenaustausch zwischen Client und Server 419
30.2.1 Sichere Kommunikation..... 419
30.2.2 Zu erwartende Netzlast..... 421
30.2.3 Intervall für Datenaustausch zwischen Client und Server definieren 422

30.3 Installation 424
30.3.1 SafeGuard Easy Server/Datenbank installieren 426
30.3.2 SafeGuard Easy Administrationskonsole installieren..... 428
30.3.3 SafeGuard Easy Clients installieren..... 429
30.3.4 Maximale Kapazität der SafeGuard Easy Datenbank..... 432
30.3.5 SafeGuard Easy Server/Datenbank wiederherstellen 432

30.4 Microsoft SQL Server-Unterstützung..... 434
30.4.1 Wichtige Hinweise..... 434
30.4.2 Leere SafeGuard Easy-Datenbank auf dem SQL-Server erzeugen..... 435
30.4.3 Neue (leere) SafeGuard Easy-Datenbank auf dem SafeGuard Easy Server registrieren . 440

31 Administrationskonsole 447

31.1 Anmelden an die SafeGuard Easy Datenbank ... 447
31.1.1 Verbindung trennen und wiederaufnehmen . 448
31.1.2 Standardzugangsdaten zur SafeGuard Easy Datenbank ändern 449

31.2 Benutzeroberfläche 452
31.2.1 Inhalt der Registerkarten als Textdatei speichern 454

31.3 Aktuelle Konfiguration eines registrierten SafeGuard Easy Clients anzeigen 455
31.3.1 Beschreibung des Client ändern 456
31.3.2 Client löschen 456

31.4 SafeGuard Easy Client neu registrieren 457
31.4.1 Mehrere SafeGuard Easy Clients neu registrieren..... 461

31.5 SafeGuard Easy Clients auf einem anderen SafeGuard Easy Server registrieren 462

31.6 Gruppen definieren 467
31.6.1 Gruppen erstellen / löschen 467
31.6.2 SafeGuard Easy Client einer Gruppe zuweisen / aus einer Gruppe entfernen..... 468
31.6.3 Gruppenzugehörigkeit..... 469
31.6.4 Gruppennamen ändern..... 470
31.6.5 Gruppe löschen 470

31.7 Filter definieren..... 471
31.7.1 Filter konfigurieren..... 471
31.7.2 Filter aktivieren..... 473

31.8 Requests und Warteschleifen 474
31.8.1 Requests erstellen 475
31.8.2 Neuen Request erstellen..... 476
31.8.3 Bestehende Konfigurationsdatei als Request verwenden 477
31.8.4 Fehlgeschlagene Requests..... 478
31.8.5 Requestnamen ändern..... 479
31.8.6 Request löschen 479
31.8.7 Warteschleife anzeigen 479

31.9 Status eines SafeGuard Easy Clients..... 481
31.9.1 Status „Standard (Online)“ 482
31.9.2 Status „Offline“ 483
31.9.3 Status „Push [ein]“..... 484
31.9.4 Status „Push [aus]“ 486

31.9.5 SafeGuard Easy Client in den OFFLINE Modus schalten 486
31.9.6 Konfigurationsupdates für Offline Clients in der Administrationskonsole erzeugen 488
31.9.7 Konfigurationsupdate auf Offline Client einspielen mit SGETRANS 491

31.10 Systemkern automatisch sichern 492
31.10.1 Systemkern eines SafeGuard Easy Clients im Verzeichnis BACKUPS ablegen 493
31.10.2 Neues Backup-Verzeichnis angeben 494
31.10.3 Systemkernsicherung exportieren 495

32 Remote Administration 497

32.1 Voraussetzungen 498

32.2 Installieren der Remote Administration 500

32.3 Verbindung zu einem SafeGuard Easy Client aufbauen 502

33 Fehlermeldungen 505

1 Überblick

Personalcomputer enthalten häufig personenbezogene Daten, vertrauliche und interne Firmeninformationen oder andere sensible Daten. Nicht zu unterschätzen ist die Gefahr, die durch den Diebstahl von Notebooks ausgeht. Hochsensible Kundeninformationen auf dem Notebook eines Vertriebsmitarbeiters könnten so z.B. an Wettbewerber gelangen und dem eigenen Unternehmen Schaden zufügen. Wer sich vor solchen Risiken schützen möchte, ohne viel Zeit in die Implementierung von Sicherheitsmaßnahmen zu investieren, findet in SafeGuard Easy die ideale Lösung.

Wie schützt SafeGuard Easy nun die Arbeitsstationen vor unbefugtem Zugriff? Die zentralen Sicherheitsfunktionen des Programms sind die Verschlüsselung von Daten und der Schutz vor Angreifern, die einen Rechner mit Hilfe eines externen Mediums starten wollen.

Die größten Vorteile von SafeGuard Easy bestehen darin, dass das Programm

- einfach, aber effektiv die Vertraulichkeit von abgespeicherten Daten sichert.
- sich schnell implementieren lässt.
- eine hohe Benutzerfreundlichkeit aufweist.
- ein für viele Anwendungsbereiche geeignetes Sicherheitskonzept bietet.

SafeGuard Easy ist einfach zu installieren und erfordert kaum Verwaltungsaufwand. Daher eignet es sich insbesondere für Einzelplatzsysteme und mobile Geräte wie Notebooks.

1.1 Zentrale Sicherheitsfunktionen

Verschlüsselung

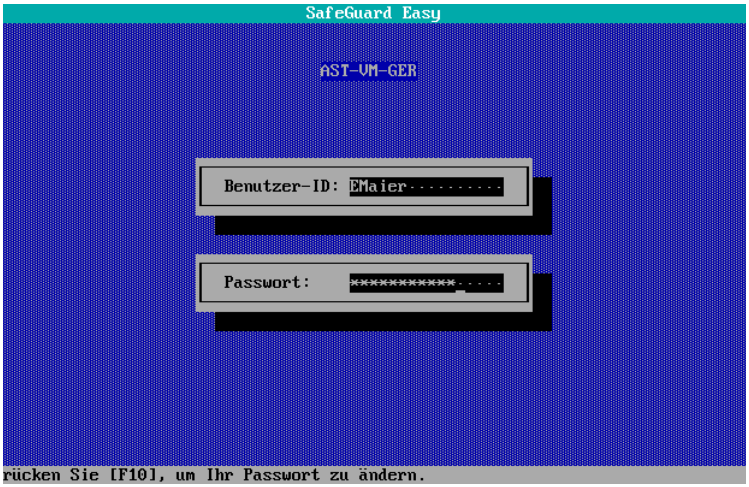
SafeGuard Easy schützt auf einfache und effektive Weise die Vertraulichkeit von Daten bei der Speicherung auf Festplatten, Disketten und Wechselmedien durch Online-Verschlüsselung. Online bedeutet in diesem Zusammenhang, dass die Daten zum Lesezeitpunkt entschlüsselt in den Arbeitsspeicher geladen und beim Schreiben automatisch wieder verschlüsselt werden. Der Schlüssel ist nicht auf der Festplatte oder im PC gespeichert. Er wird jedesmal beim Start aus dem SafeGuard Easy-Passwort des Benutzers ermittelt.

SafeGuard Easy verschlüsselt nicht nur den gesamten Inhalt von Festplatten, sondern auch von Wechselmedien wie USB-Speichersticks, Disketten, ZIP- oder JAZ Medien. Damit lässt sich ein gesicherter Datenträgeraustausch innerhalb des Unternehmens realisieren und gleichzeitig der Inhalt mobiler Datenträger gegen Unbefugte schützen. Darüber hinaus kann so auch der unbefugte Datenimport von nicht lizenzierter Software oder Viren über diesen Weg verhindert werden, da Benutzer ohne das passende Recht keine Klartextmedien verwenden können.

Für die Verschlüsselung können unterschiedliche Algorithmen für Disketten, Wechselmedien und Festplatten gewählt werden.
Zur Verfügung stehen AES, Rijndael, XOR, STEALTH-40, IDEA, BLOWFISH, DES und 3DES.

Zugangskontrolle mit Pre-Boot Authentisierung und Bootschutz

Bei der Pre-Boot Authentisierung handelt es sich um eine weitere zentrale Sicherheitsfunktion von SafeGuard Easy. Die Pre-Boot Authentisierung erlaubt nur die Anmeldung der auf dem System registrierten SafeGuard Easy Benutzer.



Wird bei verschlüsselter Festplatte versucht, den Rechner von einem anderen Medium wie z.B. einer Systemdiskette, einer CD-ROM oder einer weiteren Festplatte zu starten, bleibt die Festplatte gesperrt. Dies bedeutet, der Systemstart ist zwar möglich, die verschlüsselten Daten auf der Festplatte können aber nicht gelesen werden.

Wird die Pre-Boot Authentisierung auf einer Arbeitsstation in Verbindung mit der Option Bootschutz eingesetzt, ist es nicht möglich, die Arbeitsstation mit einem externen Medium zu starten ohne die korrekten SafeGuard Easy-Benutzerdaten zu kennen.

1.2 Weitere Sicherheitsfunktionen

Unterstützung von Lenovos (IBMs) Thinkvantage Technologien - Client Security Solution (CSS) 8.10 und Rescue and Recovery 4.20
SafeGuard Easy unterstützt diese und frühere Versionen von Lenovos Thinkvantage Technologien und ist kompatibel zu Lenovos Client Security Solution (CSS) und Rescue and Recovery (RnR).

- ***Rescue and Recovery (RnR):*** SafeGuard Easy ist kompatibel mit Rescue and Recovery. Das erlaubt Benutzern, Lenovos effiziente Backup- und Restore-Methode zu nutzen, auch wenn die Betriebssystem-Partition mit SafeGuard Easy verschlüsselt ist. SafeGuard Easy bietet hier eine einzigartige Funktionalität unter Produkten zur Festplattenverschlüsselung. Sicherungen von verschlüsselten SafeGuard Easy-Systemen können auf allen von Rescue and Recovery angebotenen Laufwerken abgelegt werden. Im Notfall ist es also möglich, ein beschädigtes System durch das Einspielen eines Backups von CD/DVD, Netzlaufwerk, einer zweiten internen Festplatte, sowie von USB-Festplatte oder -Stick wiederherzustellen.

- ***TCPA / TPM Unterstützung (ESS Chip/CSS):*** SafeGuard Easy ist das erste Produkt zur Festplattenverschlüsselung, welches die in modernen Notebooks integrierten Sicherheitschips einbindet, die von der Trusted Computing Group (TCG) spezifiziert wurden. Unter anderem nutzt SafeGuard Easy den Chip zur Sicherung der Verbindung zwischen Client und Administrationsserver, sowie zur Erzeugung von Zufallszahlen. Die SafeGuard Easy SAL-Funktion lässt sich selbstverständlich auch nutzen und stellt damit eine optimale Integration in die ESS Chip Infrastruktur dar.

Zertifizierung nach FIPS 140-2 Level 1
SafeGuard Easy erfüllt die Richtlinien der FIPS 140-2 Level 1 (FIPS = Federal Information Processing Standard)-Zertifizierung des amerikanischen National Institute of Standards and Technology (NIST). Das NIST bestimmt die Sicherheitskriterien für Verschlüsselungsprodukte der US-amerikanischen Regierung.

SafeGuard Easy ist bereits zertifiziert nach den Standard Common Criteria, Evaluation Assurance Level 3 (EAL3).

Optionale Zwei-Faktor-Authentisierung in der Pre-Boot-Phase
SafeGuard Easy kann so konfiguriert werden, dass nur Anwender mit passendem Token Zugriff auf den PC erhalten. Der Token kann nicht nur in der Pre-Boot Authentisierung, sondern natürlich über den PKCS#11 bzw. CSP Standard auch auf Betriebssystemebene für weitere, zertifikatsbasierte Anwendungen verwendet werden. Auch die Anmeldung des SafeGuard Easy Administrators an den Verwaltungsprogrammen kann selbstverständlich über den Token erfolgen. Benutzern, die ihren Token vergessen haben, hilft ein zentraler Helpdesk (Challenge/Response-Verfahren).

SafeGuard Easy unterstützt diverse Aladdin eToken, den Verisign USB-Token und den RSA SecurID 800 Token.

Biometrische Anmeldung mit Lenovo Fingerabdruck-Leser
SafeGuard Easy unterstützt neben der Anmeldung mit USB-Token (RSA, Aladdin) die Anmeldung per "Fingerabdruck" in der Pre-Boot Authentisierung. Vorteil des Fingerabdrucks ist, dass sich ein Benutzer weder SafeGuard Easy-Passwörter noch die PIN eines USB-Tokens merken muss. Er identifiziert sich z. B. an einem Lenovo Notebook einfach, indem er einen Finger über den dort eingebauten Leser führt.

SafeGuard Plug-In für Aladdins Token Management System (TMS)
Das Aladdin Token Management System ist ein auf Active Directory basierendes Werkzeug, mit dem eToken ausgestellt werden können. Ab Version 1.1 bietet das Aladdin TMS die Möglichkeit, Plug-Ins von Drittherstellern zu integrieren. Utimaco stellt so ein Plug-In zur Verfügung, über das SafeGuard Easy- (PBA-) Daten und Windows auf den eToken geschrieben werden können. Die Kombination von Aladdins TMS und Utimaco Plug-In macht die SafeGuard Token Administration für das Ausstellen von eToken überflüssig, beide Programme können aber parallel verwendet werden. Das SafeGuard TMS Plug-in muss separat bestellt werden. Eine 10 Benutzer-Demo-Lizenz wird mit SafeGuard Easy ausgeliefert und steht zum Download zur Verfügung.

„Schneller Benutzerwechsel“ mit Token

Benutzer, die die Vorteile der SafeGuard Easy Token-Anmeldung nutzen, profitieren von einer weiteren Komforteinrichtung:
Wenn an Mehrbenutzer-PCs das SafeGuard Easy-Rechteprofil zu wechseln ist (z.B. das Recht „Wechselmedienverschlüsselung abschalten“), melden Token-Benutzer sich lediglich von Windows ab. Der komplette Neustart des PCs samt Neuanmeldung in der Pre-Boot Authentisierung - wie sonst üblich - entfällt.

Hinweis: Der schnelle SafeGuard Easy-Benutzerwechsel ist nicht zu verwechseln mit dem gleichnamigen Microsoft Feature!

Hibernation (Suspend to Disk) Unterstützung

Gerade mobile Anwender nutzen gerne die Möglichkeiten moderner Betriebssysteme, den Bootvorgang durch einfaches „Pausieren“ und späteres „Wiederherstellen“ der aktuellen Arbeitssituation zu ersetzen.
Im Gegensatz zu den meisten anderen Festplattenverschlüsselungsprodukten erlaubt SafeGuard Easy, den Hibernation Modus zu nutzen und dabei sogar die erzeugten Image-Daten zu verschlüsseln. Somit bleibt die Sicherheit allzeit gewahrt, der Strombedarf wird gesenkt und die Anwender sparen Zeit gegenüber dem sonst üblichen, normalen Bootvorgang.

Kompatibilität zur Computrace Software

Computrace sorgt dafür, dass sich ein gestohlener Rechner per Netzwerk wieder meldet und seinen Standort preisgibt. Durch die Kompatibilität funktioniert das auch mit verschlüsselten Festplatten. SafeGuard Easy ist für die Zusammenarbeit mit Computrace vorbereitet. Für eine vollständige Kompatibilität ist allerdings eine Computrace Version nötig, die von Absolute Software zum jetzigen Zeitpunkt (12/2008) noch nicht freigegeben wurde.

Web Self Help

Benutzer können sich mit dem webbasierten Self Help selbst helfen, wenn sie ihr SafeGuard Easy Passwort vergessen haben. Der „Selbsthilfe“-Mechanismus verringert die Anzahl der Helpdesk-Anrufe, die sich ausschließlich mit dem Zurücksetzen vergessener Passwörter beschäftigt. Das Helpdesk-Personal hat somit mehr Zeit sich mit weniger trivialen Supportfällen zu beschäftigen. Zusätzlich sind weitere software- und hardwarebasierende Challenge/Response-Lösungen verfügbar.

Die webbasierte Passwort-Selbsthilfe ist als separates Add-on erhältlich.

Umfangreiche Passwort-Regeln
SafeGuard Easy bietet eine Vielzahl von Optionen zur Durchsetzung spezieller Passwort-Regeln in der Pre-Boot Authentisierung, z.B. eine konfigurierbare Liste verbotener Passwörter, erweiterte Regeln für Sonderzeichen, Passwort, UID etc. Firmeninterne Regelvorgaben können sehr gut abgebildet werden.

Protokollierung in Pre-Boot Authentisierung und Betriebssystem
SafeGuard Easy protokolliert sicherheitsrelevante Ereignisse, wie zum Beispiel fehlgeschlagene Anmeldeversuche, in der Pre-Boot- Phase und leitet diese später an die Windows Ereignisanzeige oder optional über eine Zusatzkomponente an einen zentralen Server zur Auswertung weiter. Somit können Angriffe schneller erkannt und Zustände einfacher diagnostiziert werden.

Optionale zentrale Administrationsdatenbank
Neben der bewährten Verteilung von Konfigurationsdateien steht als weitere Option eine eigene, zentrale Administrationssoftware für SafeGuard Easy zur Verfügung, die Systemkernsicherungen, Verteilung von Konfigurationsdaten und die Integration von Offline Clients übernimmt. SafeGuard Easy unterstützt als Standard-Datenbanktyp neben Microsoft Access auch den Microsoft SQL Server, um Informationen über SafeGuard Easy Clients zu speichern.

Die zusätzlich verfügbare „Remote Administration“ erlaubt darüber hinaus einen einzelnen Clients über das Netzwerk direkt zu konfigurieren.

Vereinfachte Konfiguration bei der zentralen Administration
Bestimmte Windows-Servicepacks verlangen zusätzliche Einstellungen für den Verbindungsaufbau zwischen SafeGuard Easy-Client und zentralem Administrationsserver. Eine neue Applikation setzt die notwendigen Einstellungen automatisch und vereinfacht die Konfiguration von Client und Server. Applikation und Beschreibung sind im Verzeichnis Tools\DCOMWizard auf der CD zu finden.

Gemeinsames Benutzer-Passwort für SafeGuard Easy und Windows (Passwortsynchronisierung)

Anrufe wegen vergessener Benutzerpassworte gehören für viele Support-Mitarbeiter zum Alltag. Eine Regel lautet: Je weniger Passworte sich ein Benutzer merken muss, desto mehr wird der Support entlastet. SafeGuard Easy trägt über eine Passwort-Funktionalität seinen Teil zur Verringerung von Benutzeranfragen bei, denn die Software lässt sich so konfigurieren, dass Windows- und SafeGuard Easy Passwort nach einem Mausklick übereinstimmen. Benutzer melden sich nach der erfolgreichen Synchronisierung mit dem gleichen Passwort an SafeGuard Easy in der Pre-Boot Authentisierung und am Betriebssystem an.

Sichere Wake On LAN-Unterstützung

Die Pre-Boot Authentisierung von SafeGuard Easy bietet optimalen Schutz gegen Hackerangriffe. Um dennoch Softwareverteilung über Wake On LAN bei aktiver Festplattenverschlüsselung auf möglichst sichere Weise zu gewährleisten, bietet SafeGuard Easy spezielle Funktionen an.

Sichere Fernwartung (Challenge/Response)

Helpdesk-Mitarbeiter können Benutzern helfen, wenn diese ihr Passwort vergessen haben. Das Challenge/Response-Verfahren ist sicher und ideal für mobile Anwender, da dabei der PC keine direkte Online-Verbindung mit dem Helpdesk benötigt.

Challenge/Response für PDA

SafeGuard Easy Benutzer, die Passwort oder Token vergessen haben, sind mit Hilfe eines zentralen Helpdesk rasch wieder produktiv. Die Helpdesk Mitarbeiter können ihre Arbeit auch mit Hilfe eines PDA (Pocket PC) mobil erledigen und sind nicht mehr auf Zugang zu einem PC angewiesen.

Windows Installer basierte Installation

Die komplett auf dem aktuellen Windows Installer (MSI) Standard basierende Installation lässt sich einfach und effizient im Windows Netzwerk verteilen und installieren.

Integrierter Boot Manager (Twinboot)

Es ist eine häufige Anforderung, die Festplatte eines Notebooks aufzuteilen: In eine vom Benutzer verwaltete ungeschützte Partition und eine vom Unternehmen verwaltete, verschlüsselte Partition. SafeGuard Easy bringt dafür einen integrierten Boot Manager mit, der es ermöglicht, solche oder ähnliche Szenarien einfach und sicher, zentral gesteuert zu realisieren. Damit bleiben die Firmendaten geschützt und der Anwender hat auf seiner privaten Partition absolute Freiheit, bis hin zur Wahl des Betriebssystems.

Verschlüsselung von USB Speichermedien und laufwerksbezogene Verschlüsselung von Wechselmedien

SafeGuard Easy unterstützt die aktuelle Generation von Plug&Play Speicherkarten (USB Speichermedien), womit auch diese für den gesicherten Datenaustausch verwendet werden können. Darüber hinaus kann die Verschlüsselung eines Disketten- oder Wechselmedien-Laufwerks temporär für jedes einzelne Laufwerk gesondert an- bzw. abgeschaltet werden.

Flexible Benutzerführung bei der Pre-Boot Authentisierung

Es lässt sich bei der Pre-Boot Authentisierung ein vom Administrator vorgegebener Hinweis auf rechtliche Belange, Eigentümer des Geräts o. ä. anzeigen.

Konfigurationsdateien aus älteren Versionen (ab SafeGuard Easy 3.20) wieder verwenden

Unternehmen setzen SafeGuard Easy Konfigurationsdateien ein, wenn eine Vielzahl an Clients eine identische SafeGuard Easy-Konfiguration erhalten soll. SafeGuard Easy importiert die „alten“ Konfigurationsdateien und übernimmt so auf einfache Weise Einstellungen und Schlüssel bei einem Upgrade ohne diese neu eingeben zu müssen.

Notfallstart von Diskette und CD

PC-Systeme werden heutzutage statt mit Diskettenlaufwerken mit CD/DVD-Laufwerken ausgestattet. SafeGuard Easy passt sich diesen Entwicklungen im Hardware-Bereich an und unterstützt als Notfallmedien neben Disketten auch CDs. Es können dabei sowohl MS DOS als auch Windows PE Bootmedien verwendet werden.

Standard Windows-Anmeldung statt SafeGuard-Dialog

Nach einer SafeGuard Easy-Installation erscheint zur Anmeldung an das Betriebssystem der reguläre Windows-Dialog. Kunden können das Erscheinungsbild der Standard-Anmeldung jedoch auch anpassen und die reguläre Windows-Anmeldung gegen einen Dialog im Utimaco-Design austauschen.

Kompatibilität mit dem Volumenschattenkopie-Dienst von Windows XP

Der Volumenschattenkopie-Dienst von Windows XP erstellt einen „Sofort-Backup“ von geöffneten Dateien oder Datenbanken. Mitarbeiter müssen ihre Arbeit also nicht unterbrechen, während ein Administrator ihre Daten sichert. SafeGuard Easy unterstützt den Volumenschattenkopie-Dienst vollständig, manuelle Systemkonfigurationen sind nicht notwendig.

Hinweis: Als Alternative zur Kopierfunktion von Windows XP können Benutzer auch andere SafeGuard Easy kompatible Tools wie Lenovos Rescue und Recovery verwenden (das auch für Nicht-Lenovo-Plattformen verfügbar ist).

1.3 Neues in SafeGuard Easy

Die Version 4.50 von SafeGuard Easy behebt in den Vorgängerversionen aufgetretene Probleme. Details entnehmen Sie bitte der Liesmich.txt.

Neues in SafeGuard Easy 4.50

Unterstützung der aktuellesten Betriebsystem Service Releases
Der SafeGuard Easy Client unterstützt die aktuellsten Version von eingesetzten Betriebssystemen, z. B. Windows XP Service Pack 3 und Windows Server 2003 Service Pack 2.

Unterstützung der aktuellesten Token Hardware und Middleware
SafeGuard Easy unterstützt die aktuellsten Versionen von Aladdin (CardOS) und RSA (SID800) Hardware und Middleware.

SafeGuard Easy unterstützt auch den Aladdin NG-Flash USB Token. Der Token kann - wie andere Token von Aladdin, Verisign und RSA, zur Authentisierung des Benutzer in der SafeGuard Easy Pre-Boot Authentication (PBA) sowie in Managementanwendungen verwendet werden.

SafeGuard Easy 4.50 ist mit dem RSA Datenformat SID800 kompatibel.

Optionale Installation der SafeGuard Easy Protokollierung
Das SafeGuard Easy Modul Logging wird nicht mehr standardmäßig während der Installation des SafeGuard Easy Client installiert. Dieses Feature kann nun als optionales Feature bei der Einrichtung des SafeGuard Easy Client unter Administrationswerkzeuge ausgewählt werden.

Verschiedene Optimierungen
Version 4.50 bietet verschiedene Optimierungen, zum Beispiel:

Das Setup fragt das Betriebssystem ab. Handelt es sich um Windows Vista, so kann die Installation nicht erfolgen. Für Windows Vista ist SafeGuard Enterprise als Sicherheitslösung vorzuziehen.

Das Tool RepPBA.exe wird auf der SafeGuard Easy Produkt-CD mitgeleifert. Über dieses Tool lässt sich die Anmeldungsmethode innerhalb der PBA ändern, z. B. von Tastaturanmeldung zu Tokenanmeldung.

Eine vollständige Auflistung aller Optimierungen finden Sie in der Datei `Liesmich.txt`.

1.4 Änderungen zu Vorgängerversionen

USB-Token neu ausstellen

USB-Token, die mit SafeGuard Easy Versionen **vor 4.11** ausgestellt wurden, sind in der aktuellen Version nicht automatisch wiederverwendbar, da sich das Datenformat auf dem Token geändert hat. Diese „alten“ Token müssen neu ausgestellt werden, um sich wie gewohnt an der Pre-Boot Authentisierung anzumelden.

Die Ausstellung übernimmt der Benutzer i.d.R. selbst (das entsprechende SafeGuard Easy-Recht vorausgesetzt). Bei der Erstanmeldung mit Token an das neue SafeGuard Easy zeigt die Pre-Boot Authentisierung dann die Meldung „Keine SafeGuard Easy-Zugangsdaten auf dem Token, bitte stellen Sie den Token jetzt aus“ an. Diese Meldung muss Benutzer „alter“ Token aber nicht beunruhigen, sie geben einfach ihre SafeGuard Easy-Zugangsdaten in die vorgegebenen Felder ein. Sind die Daten korrekt, werden sie auf den Token geschrieben und für die nächste Anmeldung genügt wieder die Angabe der Token-PIN.

Für den Fall, dass ein Benutzer seine SafeGuard Easy-Zugangsdaten nicht kennt, kontaktiert er einen Ansprechpartner beim Support/Helpdesk. Dieser schreibt die Daten über das neue SafeGuard Easy Plug-in für die Token Administration auf den Token.

Das SafeGuard Easy Plug-in für die Token Administration ist auf der Produkt-CD im Verzeichnis \TOOLS abgelegt (SCAdmin_SGEasy.msi).

SGEInteg ersetzt CheckArea/MigHelp

Ab Version 4.30 heißt die Reparaturfunktion beim Update für den SafeGuard Easy-Systemkern "SGEInteg". SGEInteg übernimmt die Funktionalität von CheckArea/MigHelp und ist im Verzeichnis \TOOLS der Programm-CD zu finden.

1.5 Systemvoraussetzungen

Minimale Betriebssystemvoraussetzungen

- Windows 2000 Professional (Service Pack 4)
- Windows XP Home Edition (Service Pack 2)
- Windows XP Professional Edition (Service Pack 2)
- Windows 2000 Server (nur Standard Version, Service Pack 1)
- Windows Server 2003 (nur Standard Version)

Empfohlen wird für alle oben aufgeführten Betriebssysteme der aktuelle Service Pack-Stand (12/2008).

SafeGuard Easy wurde nicht getestet mit Windows XP Media Edition.

Hinweis zu Windows XP
SafeGuard Easy kann in den Versionen 4.50 kann auch unter Windows XP SP2 oder SP3 betrieben werden. Auch eine Migration, zum Beispiel von SP2 zu SP3 bei installiertem SafeGuard Easy ist möglich.

Hinweis zu Windows XP SP 2/Windows Server 2003 SP 1
Bei Verwendung des optionalen zentralen Administrationsservers bzw. der Remote Administration von SafeGuard Easy 4.x sind besondere Konfigurationseinstellungen in Windows XP SP2 und Windows Server 2003 SP 1 zu treffen.

Alle nötigen Einstellungen sind in unserer Wissensdatenbank **http://www.utimaco.de/myutimaco** im Knowledge Item „106898 SafeGuard Easy and SP2 Configuration for Windows XP“ beschrieben. Nutzen Sie die Suchfunktion, und geben Sie die Nummer „106898“ ein.

Zusätzlich ist eine Applikation vorhanden, mit der man die Konfigurationseinstellungen automatisch setzen kann, um die zentrale Administration und die Remote Administration mit Windows XP Service Pack 2 zu nutzen. Sie finden die Applikation auf der CD im Verzeichnis Tools\DCOMWizard oder in der Wissensdatenbank. Nutzen Sie die Suchfunktion, und geben Sie „SP2“ oder „SGE" ein.

Hinweis zu Windows XP Home Edition:
SafeGuard Easy unterstützt nicht

- Sichere automatische Anmeldung mit Smartcard (Smartcard-SAL)
- Zentrale Protokollierung

Hinweis zu Windows Server Edition:
SafeGuard Easy unterstützt nicht

- SMP
- 64-Bit-Server

Unterstützte Dateisysteme

- FAT-12
- FAT-16
- FAT-32
- HPFS
- NTFS
- NTFS5

Unterstützte Speichermedien

- Festplatten (IDE, SCSI, Serial-ATA, Firewire, USB)
- Disketten
- Wechselmedien wie ZIP/JAZ
- USB Speichersticks
- RAID 0 (Hardware-RAID)

  SafeGuard Easy unterstützt nicht:
  - weitere RAID-Klassen
  - Software-RAID 0

Unterstützte Prozessoren

- AMD
- Intel
- Multi-Prozessor / Hyperthreading
  SafeGuard Easy 4.x wurde erfolgreich sowohl auf Multi-Prozessor Rechnern wie auch auf Rechnern mit Hyperthreading (Bsp. Pentium IV) getestet und installiert.

Hardwareanforderungen

- **Festplattenspeicherplatz**
  Abhängig von der gewählten Installationsmethode benötigt SafeGuard Easy Festplattenspeicher zwischen minimal fünf und maximal 25 MB. SafeGuard Easy hat die gleichen Mindestanforderungen wie das eingesetzte Betriebssystem.

  Obwohl SafeGuard Easy auf dem beschriebenen System einwandfrei läuft, hat Verschlüsselung ihren Preis. Es wird deshalb empfohlen, Hardware zu verwenden, die über die genannten minimalen Anforderungen hinausgeht.

- **Anzahl der Festplatten**
  SafeGuard Easy unterstützt maximal 4 Festplatten mit maximal 8 Partitionen pro Festplatte. Es wird eine Warnung ausgegeben, wenn ein nicht unterstützter Partitionstyp gefunden wird.

1.6 Dokumentation

SafeGuard Easy wird mit diesem Handbuch und der Onlinehilfe SGEasy0407.chm ausgeliefert.

1.7 Allgemeine Hinweise

- Die Funktion „Schneller Benutzerwechsel“ von Windows XP wird von SafeGuard Easy nicht unterstützt. Nach der Installation von SafeGuard Easy wird der Willkommen-Bildschirm automatisch abgeschaltet.
- Wenn der PC in ein Peer-to-Peer LAN integriert ist, dürfen Teile von Festplatten nicht für andere Benutzer dieses LAN freigegeben werden.
- Festplattenver- und -entschlüsselung sind automatisch gegen Stromausfälle u.ä. abgesichert. Bei Wiederherstellung der Stromversorgung wird der Vorgang ohne Benutzereingriff automatisch an der richtigen Stelle fortgesetzt.

HINWEIS:
Die Erstverschlüsselung von hot-pluggable Festplatten darf nicht unterbrochen werden.

- Bei kurzzeitigem Verlassen des PC sollte die Windows-Bildschirmsperre (Schaltfläche [Arbeitsstation sperren]) aktiviert, bei längerer Abwesenheit der PC ausgeschaltet bzw. neu gebootet werden.

- Bei korrekter Einstellung der empfohlenen Systemkonfiguration wird der logische Zugriff auf Festplatten nach dem Booten von Diskette verhindert. Um einen zusätzlichen Schutz des Systems gegen das Ausspähen eines SafeGuard Easy Passworts durch ein „Trojanisches Pferd“-Programm zu erzielen, sollte der PC gegen das Booten von der Diskette durch eine mechanische Sperre oder eine systeminterne Maßnahme geschützt werden.

1.8 Lizenzhinweise

Jede unerlaubte Vervielfältigung des Handbuchs sowie der Software von SafeGuard Easy wird strafrechtlich verfolgt. Sie dürfen SafeGuard Easy nur auf einem PC installieren.

Falls Sie die Sicherheitskopie dazu missbrauchen, um SafeGuard Easy auf mehreren PCs zu installieren, verstoßen Sie gegen die Lizenzbestimmungen und machen sich strafbar. Wollen Sie mehrere PCs schützen, muss für jeden PC eine Lizenz erworben werden.

Es gelten die Bedingungen des Software-Lizenzvertrages.

Weitere Lizenzhinweise

STEALTH Encryption Copyright (c) 1994 Intelligence Quotient International Limited. All rights reserved. Patents pending. STEALTH encryption is a trademark of Intelligence Quotient International Limited.

Patent rights of Ascom Tech Ltd. given in EP, JP, US. IDEA is a trademark of Ascom Tech Ltd.

Danksagungen

Besonderer Dank gilt Dr. Brian Gladman, dessen AES-Implementation wir als Basis für unsere AES-Verschlüsselungstreiber verwendet haben.

2 Erste Schritte

Dieses Kapitel erklärt die notwendigsten Voraussetzungen für eine erfolgreiche Installation von SafeGuard Easy.

2.1 Installation vorbereiten

Um SafeGuard Easy so effektiv wie möglich einzusetzen, müssen bereits vor der Installation umfangreiche Vorkehrungen getroffen werden. Lesen Sie die nachfolgende Auflistung bitte sorgfältig durch und vergewissern Sie sich, dass Sie alle Punkte berücksichtigt haben.

- Erstellen Sie bitte vor der Installation von SafeGuard Easy einen kompletten Backup Ihrer Datenträger.
- Alle Festplatten, die verschlüsselt werden sollen, müssen bei der Installation von SafeGuard Easy bereits mit dem PC verbunden und eingeschaltet sein.
- Die Partitionen Ihrer Festplatte sollten vollständig formatiert und einem Laufwerksbuchstaben zugeordnet sein.
- Wechselmedienlaufwerke oder USB Speichersticks müssen nicht am PC angeschlossen sein, wenn SafeGuard Easy installiert wird.
- Untersuchen Sie die Festplatte(n) auf Fehler (Chkdsk).

  Weitere Informationen zu diesem Thema erhalten Sie in der Utimaco-Wissensdatenbank
  http://www.utimaco.de/myutimaco.
  Nutzen Sie bitte die Suchfunktion der Wissensdatenbank, um nach Stichworten wie „Dateisystem“ oder „NTFS“ zu suchen.
- Schalten Sie bitte alle aktiven Virenscanner für die Dauer der Installation/Deinstallation aus (noch besser ist eine Deinstallation).
- Wenn Sie einen Bootmanager benutzen, ziehen Sie eine Neuinstallation des Systems ohne Bootmanager in Betracht.

- Wenn die Daten mit Hilfe eines Clone-Tools (Drive Image, Ghost) auf die Festplatte gebracht wurden, empfehlen wir den MBR „neu“ zu schreiben.

  Die Installation von SafeGuard Easy benötigt einen „einwandfreien“ Master Boot Record und dieser könnte eventuell durch Image/Clone Programme nicht mehr in diesem Zustand sein.

  Säubern Sie den Master Boot Record, indem Sie von Diskette, CD oder DVD booten (identisches System wie auf der Festplatte empfohlen) und fdisk /MBR ausführen.

- Wenn die Bootpartition von FAT nach NTFS konvertiert wurde, der Systemabschluss mit einem Neustart aber noch nicht durchgeführt wurde, sollte SafeGuard Easy nicht installiert werden. Hierbei ist es möglich, dass die Installation nicht beendet wird, da das Dateisystem zum Zeitpunkt der Installation noch FAT ist, jedoch zum Zeitpunkt der Aktivierung NTFS vorgefunden wird. In diesem Fall müssen Sie einmalig neu starten, bevor SafeGuard Easy installiert wird.

SafeGuard Easy wird ständig weiterentwickelt. Daher kann Ihre Version bereits Neuerungen enthalten, die bei Redaktionsschluss des Handbuches bzw. der Online-Hilfe noch nicht berücksichtigt werden konnten. Diese Änderungen sind in der Datei `Liesmich.txt` beschrieben.

2.2 Installationsvoraussetzungen

Für die Installation von SafeGuard Easy müssen verschiedene Voraussetzungen auf einer Arbeitsstation erfüllt sein:

- **Microsoft Windows Software Installer (MSI) v2.0**
  - Bei Windows XP standardmäßig vorhanden.
  - Bei Windows 2000 vorhanden ab Service Pack 3 oder höher.

- **High Encryption Package (nur für zentrale Administration mit SafeGuard Easy Datenbank notwendig)**
  Die zentrale Administration über SafeGuard Easy Datenbank und SafeGuard Easy Server verlangt, dass Windows die Verschlüsselung mit 128 bit Schlüsseln unterstützt.
  - Bei Windows XP standardmäßig installiert.
  - Bei Windows 2000 ab Service Pack 2 installiert.

2.3 Installierbare Module

SafeGuard Easy setzt sich aus verschiedenen sogenannten „Modulen" zusammen, die voneinander unabhängig arbeiten.

Die verschiedenen Module sind in Form von MSI-Paketen auf der Produkt-CD im Verzeichnis SGEASY\INSTALL unter CLIENT, SERVER und RUNTIME abgelegt. In den Unterverzeichnissen befinden sich, sortiert nach Sprache die notwendigen Dateien.

Diese Module sind verfügbar:

`SGEasy.msi`	Client-Applikation für SafeGuard Easy
`Runtime.msi`	Laufzeitsystem
`Server.msi`	SafeGuard Easy Server Komponente

SafeGuard Easy, das Laufzeitsystem und der SafeGuard Easy Server werden als verschiedene Produkte installiert und erscheinen demzufolge auch separat in der Liste der vorhandenen Software auf einem System.

2.4 Sprache der Benutzeroberfläche

Startet man die Installation über „Setup.exe“, ist die Sprache der Benutzeroberfläche während und nach der Installation von SafeGuard Easy abhängig von den unter Systemsteuerung / Ländereinstellungen eingestellten Regions- und Sprachoptionen. SafeGuard Easy unterstützt Deutsch, Englisch und Französisch. Wenn z.B. als Gebietsschema „Deutsch“ eingestellt ist, erscheint die Benutzeroberfläche in Deutsch, gleiches gilt für „Englisch“ und „Französisch. Die Online-Hilfe ist immer in jener Sprache verfügbar, die bei der Installation ausgewählt war. Die Änderung der Regions- und Sprachoptionen beeinflusst die Sprache der Online-Hilfe nicht.

Startet man die Installation über eine msi-Datei, ist die Sprache der Benutzeroberfläche immer Englisch. Um andere Sprachen (Deutsch/ Französisch) zu unterstützen, müssen sogenannte “Transforms„ durchgeführt werden.

Der Windows Installer nutzt Transformierungs-Dateien, um das Installationspaket automatisch auf die neue Sprache umzuschalten. Derzeit gibt es folgende Transformierungs-Dateien:

`Sgeasy_g.mst` (für Deutsch) und `Sgeasy_f.mst` (Französisch)

Um also angepasste Texte während der Installation zu erhalten, führen Sie folgendes Kommando aus:

```
msiexec /I <Msi-Package> TRANSFORMS=<Transformierungsdatei>
```

Eine deutschsprachige Installation erfordert die Ausführung der folgenden Kommandozeile:

```
msiexec /I Sgeasy.msi TRANSFORMS=Sgeasy_g.mst
```

Beachten Sie, dass der Parameter TRANSFORMS immer in Großbuchstaben geschrieben werden muss!

SGEasy.msi nutzt die Datei Setup.ini, in der zusätzliche Parameter definiert werden können, vorausgesetzt sie sind in der Syntax Cmd-Line={Parameter1, Parameter2,...} vorhanden.

Gleiches gilt für die Installation des Laufzeitsystems (Runtime.msi) und des SafeGuard Easy Servers (SGEasy.msi).

3 Lokale Installation

Bei einer lokalen Installation wird SafeGuard Easy von der Produkt-CD auf einen Stand-alone Client installiert. Die folgenden Schritte zeigen, wie man eine lokale Installation ausführt.

Der Benutzer, der SafeGuard Easy installieren will, muss mit **Windows-Administratorrechten** angemeldet sein, da hier auf die Festplatte zugegriffen werden muss bzw. Treiber und Systemdienste installiert werden, die ebenfalls Administratorrechte erfordern.

3.1 Schritt-für-Schritt-Anleitung

1. Benutzen Sie eine Programm-CD, wird die Installation nach dem Einlegen der CD in das CD-ROM Laufwerk automatisch gestartet (sollte dies nicht der Fall sein, rufen Sie die Datei **Setup.exe** aus dem Verzeichnis \CLIENT der Programm-CD auf). Ein Installationsassistent führt Sie dann durch die Installation. Klicken Sie auf [Weiter].
2. Der Dialog *Lizenzvertrag* erscheint. Wenn Sie sich mit den Lizenzbedingungen einverstanden erklären, markieren Sie das Kontrollkästchen „Ich akzeptiere den Lizenzvertrag“. Akzeptieren Sie die Lizenzbedingungen nicht, wird die Installation beendet. Klicken Sie auf [Weiter].
3. Der Dialog *Zielordner* erscheint. Geben Sie das gewünschte Installationsverzeichnis ein. Das Standard Installationsverzeichnis ist Utimaco\SafeGuard auf dem Bootlaufwerk. Ist bereits ein SafeGuard-Produkt auf der Arbeitsstation vorhanden, wird automatisch dessen Installationsverzeichnis ausgewählt.
   Benutzen Sie für den Verzeichnisnamen keine Sonderzeichen.
   Klicken Sie auf [Weiter].
4. Der Dialog *Funktionen auswählen* wird angezeigt. In diesem Dialog können Sie auswählen, welche Funktionen (Features) installiert werden sollen. Klicken Sie auf [Weiter].

   Ausführliche Informationen zu den Funktionen (Features) finden Sie in den jeweiligen Kapiteln.

   Verschlüsselung
   Installiert SafeGuard Easy komplett mit allen zur Verfügung stehenden Komponenten, wählbar sind nur

   - **Sicherer automatischer Logon (SAL)**
     Merkt sich bei der Erstanmeldung die Windows-Zugangsdaten, so dass bei jeder weiteren Anmeldung nur die SafeGuard Easy-Zugangsdaten an der Pre-Boot Authentisierung notwendig sind (siehe ’Sicherer automatischer Logon (SAL)’).

- **Server Anbindung**
  Ist für die verschlüsselte Kommunikation zwischen Client und Server unbedingt erforderlich, wenn die Arbeitsstation zentral verwaltet werden soll. Die Server-Anbindung muss nicht installiert werden, wenn die Arbeitsstation nur Stand-alone verwendet wird (siehe 'Zentrale Administration').

- **SmartCard Auto Logon**
  Leitet die Windows-Zugangsdaten einer Smartcard automatisch weiter, so dass zur Anmeldung nur die SafeGuard Easy-Zugangsdaten an der Pre-Boot Authentisierung notwendig sind (siehe 'Anmeldung an Windows mit Smartcard (Smartcard-SAL)').

- **FIPS Mode**
  Garantiert, dass SafeGuard Easy gemäß den Richtlinien von FIPS 140-2 Level 1 installiert wird (siehe 'FIPS 140-2 (Level 1) Zertifizierung').

Administrationswerkzeuge

Auf einem Administrator-PC, der ausschließlich zur Verwaltung von SafeGuard Easy Clients dient, müssen nicht alle Funktionen vorhanden sein. In der Regel genügen die Administrationswerkzeuge (Achtung: SafeGuard Easy Administration wird nicht mit den Administrationswerkzeugen installiert).
Zu den Administrationswerkzeugen zählen:

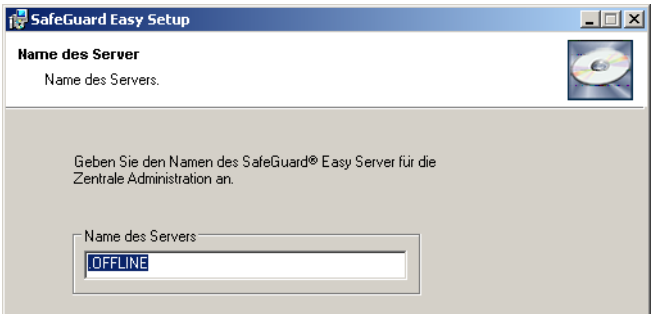
- **SafeGuard Easy Logging**
  Protokolliert sicherheitsrelevante Ereignisse, die von installierten SafeGuard Produkten ausgelöst werden. Neben der reinen Protokollierung bietet diese Funktion auch einen Filtermechanismus, der den Administrator bei der Auswahl von relevanten Ereignissen unterstützt (siehe 'Protokollierung').

- **Konfigurationsdateiassistent**
  Erzeugt Dateien, nach deren Ausführung die aktuelle Konfiguration eines Clients automatisch geändert wird, z.B. ein neuer Benutzer eingefügt wird (siehe 'Konfigurationsdateiassistent').

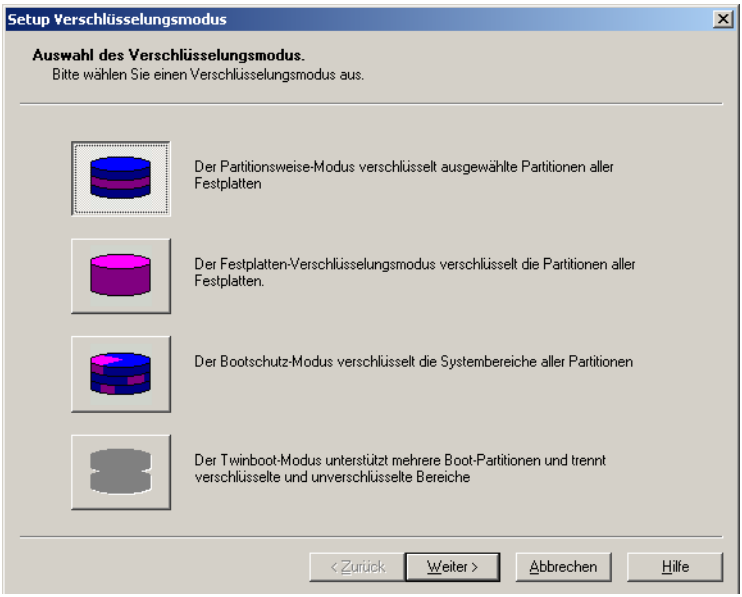
- **Response Code Assistent**
  Dient dazu, Benutzern bestimmte Aktionen zu erlauben (z.B. neues Passwort setzen), auch wenn der Administrator nicht vor Ort ist (siehe 'Fernwartung (Challenge/Response)').
- **Token-Unterstützung für Administration**
  Erlaubt, sich mit Token an die Administrationswerkzeuge (auch Administration) anzumelden (siehe 'Mit Token an den Administrationswerkzeugen anmelden').

Detaillierten Informationen zu den Installationsoptionen finden Sie in den relevanten Kapiteln.

5. Wenn Sie „Server Anbindung“ ausgewählt haben, geben Sie den Namen des zentralen SafeGuard Easy Servers an.


SafeGuard Easy Setup
Name des Server
Name des Servers.
Geben Sie den Namen des SafeGuard® Easy Server für die Zentrale Administration an.
Name des Servers
OFFLINE

6. Im nächsten Schritt legen Sie den **Verschlüsselungsmodus** für die Festplatten Ihres PCs fest.
   Weitere Details siehe 'Verschlüsselungsmodus'.

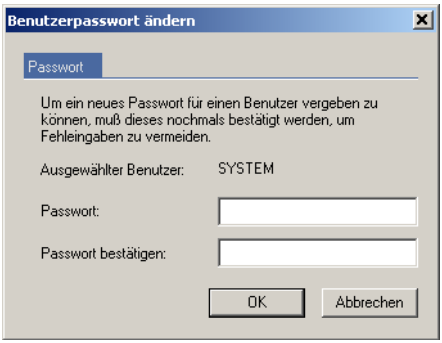

Setup Verschlüsselungsmodus
Auswahl des Verschlüsselungsmodus.
Bitte wählen Sie einen Verschlüsselungsmodus aus.
Der Partitionsweise-Modus verschlüsselt ausgewählte Partitionen aller Festplatten
Der Festplatten-Verschlüsselungsmodus verschlüsselt die Partitionen aller Festplatten.
Der Bootschutz-Modus verschlüsselt die Systembereiche aller Partitionen
Der Twinboot-Modus unterstützt mehrere Boot-Partitionen und trennt verschlüsselte und unverschlüsselte Bereiche
< Zurück
Weiter >
Abbrechen
Hilfe

7. Im nächsten Schritt folgen die Konfigurationseinstellungen.
   Eine detaillierte Beschreibung der Einstellungen finden Sie in den entsprechenden Kapiteln im Handbuch.

ACHTUNG:
Die Option **Nur mit Token** (siehe Allgemein/Authentisierung/Anmeldungsart) bedeutet, dass SafeGuard Easy die Token-Anmeldung für alle SafeGuard Easy Benutzer einer Arbeitsstation erzwingt.

Benutzer können sich in diesem Modus nur in der Pre-Boot Authentisierung anmelden, wenn auf dem Token bereits SafeGuard Easy-Zugangsdaten vorhanden sind. Mit einem „leeren“ Token ist die Anmeldung in der Pre-Boot Authentisierung nicht möglich!

8. Im nächsten Schritt werden Sie aufgefordert, Passwörter für die vordefinierten SafeGuard Easy-Benutzerprofile SYSTEM und User anzugeben. Diese Passwörter müssen den SafeGuard Easy-Passwortregeln entsprechen.



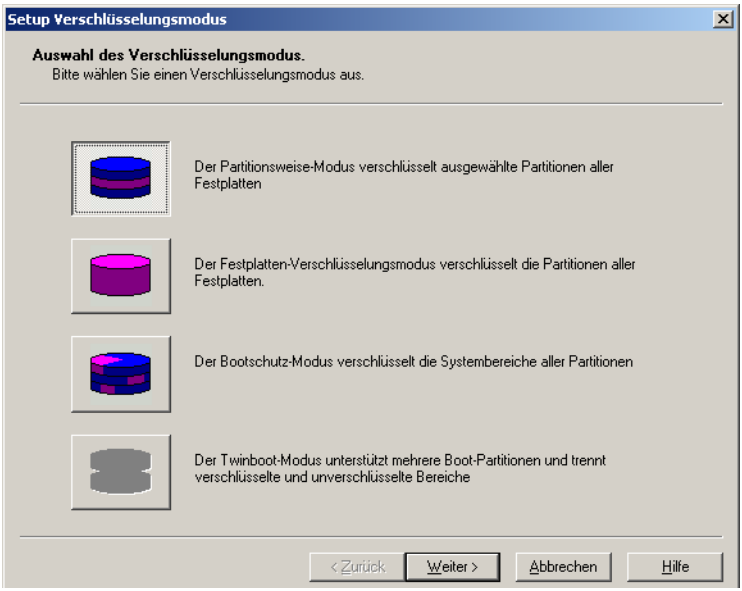
ACHTUNG:
Bitte merken Sie sich die Passwörter, die Sie hier eintragen!

Ist die Funktion "Passwort beim Systemstart abfragen" (=Pre-Boot Authentisierung) im Ordner Allgemein aktiviert, können Sie sich nach dem Neustart des PC nur mit den definierten Benutzernamen und Passwörtern anmelden!

9. Der Abschluss der Installation wird mit einem Dialog (Gratulation) angezeigt.
10. Starten Sie den PC neu.

3.1.1 Verschlüsselungsmodus

Angaben zum Verschlüsselungsmodus werden immer dann verlangt, wenn SafeGuard Easy installiert wird (manuelle Installation, Konfigurationsdatei mit der Eigenschaft Installieren).


Setup Verschlüsselungsmodus
Auswahl des Verschlüsselungsmodus.
Bitte wählen Sie einen Verschlüsselungsmodus aus.
Der Partitionsweise-Modus verschlüsselt ausgewählte Partitionen aller Festplatten
Der Festplatten-Verschlüsselungsmodus verschlüsselt die Partitionen aller Festplatten.
Der Bootschutz-Modus verschlüsselt die Systembereiche aller Partitionen
Der Twinboot-Modus unterstützt mehrere Boot-Partitionen und trennt verschlüsselte und unverschlüsselte Bereiche
< Zurück
Weiter >
Abbrechen
Hilfe

- **Partitionsweise-Modus**
  Alle ausgewählten Partitionen werden komplett verschlüsselt. Wählen Sie diese Einstellung, wenn Ihre Festplatte/n mehrere Partitionen besitzt/en, Sie allerdings nicht alle verschlüsseln wollen. Welche Partitionen zu verschlüsseln sind, entscheiden Sie später in den Verschlüsselungseinstellungen.

- **Festplatten-Verschlüsselungsmodus**
  Alle während der Installation von SafeGuard Easy angeschlossenen Festplatten werden komplett verschlüsselt. SafeGuard Easy erkennt automatisch, ob Ihr Rechner über eine oder mehrere Festplatten verfügt. Das Programm kann auf Systemen mit bis zu vier physikalischen Festplatten installiert werden und unterstützt bis zu acht logische Laufwerke/Partitionen je Festplatte.

- **Bootschutz-Modus**
  Mit dieser Option darf niemand ohne entsprechende Berechtigung den Rechner von einer Betriebssystem-Diskette/CD/DVD booten, um Zugriff auf die Festplatte eines PCs zu erhalten. Effektiver Bootschutz besteht aber nur in Verbindung mit aktivierter Pre-Boot Authentisierung.

  Der Bootschutz-Modus verschlüsselt unformatierte oder nicht bekannte Partitionen komplett.
  Bei FAT und FAT32 werden die Systembereiche verschlüsselt.
  Bei NTFS wird vom Anfang der Partition bis zum Ende der MFT (Master File Table) die Partition verschlüsselt.

- **Twinboot-Modus (wird nur bei mindestens zwei primären Partitionen angezeigt)**
  Mit dieser Option werden eine verschlüsselte und eine unverschlüsselte Partition erzeugt. Beide müssen bootfähige primäre Partitionen sein. Wird die verschlüsselte Partition gestartet, ist kein Zugriff auf die unverschlüsselte möglich und umgekehrt. Auf diese Art und Weise ist es möglich, private und geschäftliche Daten voneinander zu trennen.

  Wenn die verschlüsselte Partition gestartet wird, muss das SafeGuard Easy Passwort an der Pre-Boot Authentisierung eingegeben werden, für die unverschlüsselte besteht kein SafeGuard Easy Passwortschutz.

  Weitere Details siehe ’Twinboot/Bootmanager’.

3.2 Nach der Installation

PC neu starten

Nach der Installation (auch bei der Deinstallation) von SafeGuard Easy muss der Rechner heruntergefahren und neu gestartet werden. Auch zu diesem Zeitpunkt geöffnete Applikationen werden ohne Sicherung geschlossen. Um Datenverluste zu vermeiden, schließen sie bitte alle aktiven Anwendungen.

Pre-Boot Authentisierung erscheint nach zweitem Neustart

Nach dem ersten Neustart ist die Pre-Boot Authentisierung noch inaktiv. Zu diesem Zeitpunkt sind nur die Rechte verfügbar, die dem *AUTOUSER zugeteilt wurden. Sobald ein Windows-Benutzer sich anmeldet, den Rechner wieder herunterfährt und erneut startet, erscheint bei aktivierter Pre-Boot Authentisierung der SafeGuard Easy-Anmeldebildschirm und ein SafeGuard Easy-Benutzer kann sich anmelden.

Systemstart von Diskette

Wird der PC heruntergefahren bevor die Verschlüsselung der Festplatte beendet ist, bootet der Rechner bei jedem Neustart IMMER direkt von der Festplatte, d.h. ein Systemstart von Diskette ist nicht möglich. Dies gilt auch für den ersten Neustart nachdem die Verschlüsselung beendet ist.

Partitionierung nicht mehr ändern

Wenn die erste Festplatte ihres PCs verschlüsselt wurde (oder auch nur eine Partition), dürfen Sie die Partitionierung nicht mehr ändern. Für eine Neueinteilung deinstallieren Sie zuerst SafeGuard Easy (= Entschlüsseln der ersten Festplatte), erzeugen/entfernen Sie Partitionen und installieren Sie SafeGuard Easy erneut.

Erstverschlüsselung von "Hot-Pluggable" Festplatten nicht unterbrechen

Als "Hot-pluggable" bezeichnet man USB Geräte, die angeschlossen und abgesteckt werden können ohne das System neu zu starten. Die Erstverschlüsselung von Hot-Pluggable Festplatten darf nicht unterbrochen werden (Weitere Informationen unter Unterstützte Festplattenlaufwerke').

Dauer der Erstverschlüsselung

SafeGuard Easy benötigt für 10 GB bei der Erstverschlüsselung mit AES-256 auf einem aktuellen Notebook ca. 20 bis 30 Minuten.

Falls die Erstverschlüsselung fehlschlägt und der Computer nicht mehr gebootet werden kann, wenden Sie sich bitte an den Utimaco Support.

3.3 Verschlüsselungsfortschritt

Wurde während der Installation die Verschlüsselung der Festplatte bzw. einer Partition aktiviert, startet ein Programm, das den Verschlüsselungsfortschritt anzeigt.

Fortschritt bei Verschlüsselung eines Laufwerks

Fortschritt bei Verschlüsselung aller Laufwerke

Verschlüsselungsgeschwindigkeit

Die Verschlüsselung erfolgt im Hintergrund, d.h. der Benutzer kann während der Verschlüsselung an seinem Rechner arbeiten. Werden sehr kleine Partitionen oder nur Systembereiche verschlüsselt, kann es sein, dass der Dialog nicht angezeigt wird.

3.3.1 Verschlüsselungsfortschritt ausschalten

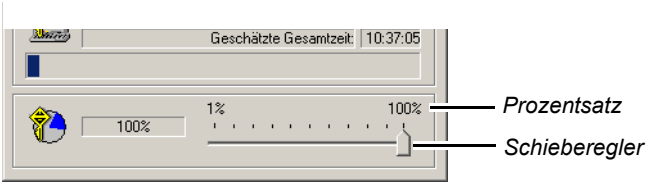
Zum Unterdrücken des Dialogs legen Sie in der Windows-Registrierung folgenden Registry Key [DWORD-Wert] neu an unter

HKEY_LOCAL_MACHINE
SOFTWARE
Utimaco
SGEasy

„**ShowECView**“=0

3.3.2 Verschlüsselungsgeschwindigkeit definieren

Die Verschlüsselungsgeschwindigkeit beträgt in der Grundeinstellung 100% und kann mit dem Schieberegler im Dialog zur Anzeige des Verschlüsselungsfortschritts verändert werden. Je höher der gewählte Prozentsatz, desto schneller wird verschlüsselt.



Änderungen der Verschlüsselungsgeschwindigkeit speichert SafeGuard Easy nicht, nach einem Neustart des PCs steht der Schieberegler wieder auf der höchsten Stufe (Standard 100%).

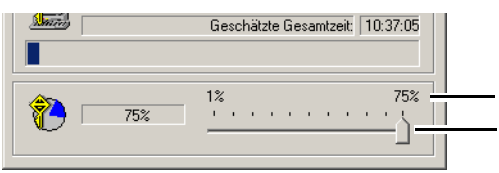
Festen Wert für Verschlüsselungsgeschwindigkeit definieren

Die Verschlüsselungsgeschwindigkeit kann so angepasst werden, dass sie bei jedem Neustart auf einen bestimmten Wert (in Prozent) gesetzt wird. Um dies zu erreichen, erzeugen Sie folgenden Registry Key [DWORD-Wert] neu:

HKEY_LOCAL_MACHINE
SOFTWARE
Utimaco
SGEasy
DefaultCPUUsage“=<Prozentwert>

Wenn der Registry Key vorhanden ist, wird die Verschlüsselung mit dem angegebenen Prozentwert beim Neustart fortgesetzt. Der Prozentwert kann jedoch nach oben und unten über den Schieberegler verändert werden.

Maximale Verschlüsselungsgeschwindigkeit definieren



Die Verschlüsselungsgeschwindigkeit kann auf einen Wert kleiner 100 Prozent begrenzt werden. Um dies zu erreichen, erzeugen Sie folgenden Registry Key [DWORD-Wert] neu und geben einen Prozentwert ein (z. B. "75"):

HKEY_LOCAL_MACHINE
SOFTWARE
Utimaco
SGEasy
„MaxCPUUsage“=<Prozentwert>

Schieberegler deaktivieren

Damit Benutzer die Verschlüsselungsgeschwindigkeit nicht ändern bzw. beeinflussen können, ist der Schieberegler zu deaktivieren. Dies geschieht über den Registry Key [DWORD-Wert]

HKEY_LOCAL_MACHINE
SOFTWARE
Utimaco
Sgeasy
„ChangeCPUUsage“

Wenn der Registry Key vorhanden und auf den Wert „0“ gesetzt ist, kann die Verschlüsselungsgeschwindigkeit nicht beeinflusst werden.

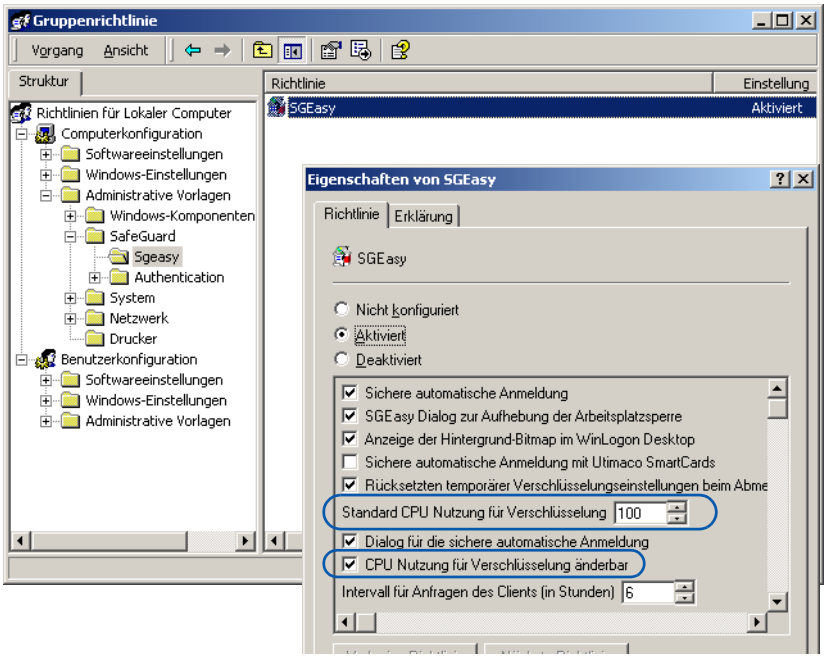
Einstellungen für Verschlüsselungsgeschwindigkeit in der administrativen Vorlage ändern

Die Einstellungen für die Verschlüsselungsgeschwindigkeit sind auch über eine Richtlinie in der administrativen Vorlage von SafeGuard Easy schaltbar (siehe 'Häufig verwendete Registry-Einstellungen für SafeGuard Easy über die administrative Vorlage ändern').

Die Richtlinie ist zu finden unter

Computerkonfiguration
\Administrative Vorlagen
\SafeGuard
\Sgeasy

Auf der Eigenschaftenseite der Richtlinie „SGEasy“ sind dafür die Optionen „Standard CPU Nutzung für Verschlüsselung“ und „CPU Nutzung für Verschlüsselung änderbar“ vorgesehen.



3.4 Hintergrund-Bitmap in der Windows-Anmeldung austauschen

Es besteht die Möglichkeit, das Bitmap anzupassen, das nach Eingabe der SafeGuard Easy-Zugangsdaten erscheint. Dies ermöglicht es Kunden, den Hintergrund von SafeGuard Easy den Bedürfnissen ihres Unternehmens anzupassen. Das angezeigte Standard-Bitmap hat den Namen **SgeLogo.bmp** und liegt **im gewählten SafeGuard Easy-Verzeichnis**. Um das Titel-Bitmap **auszutauschen**, muss nur das Standard-Bitmap mit einem angepassten Bitmap gleichen Namens und Größe ersetzt werden.

Das Bitmap hat eine Größe von 640x480 Pixel und eine maximale Farbtiefe von 8 Bit.

Wenn **KEIN Hintergrund-Bitmap** erscheinen soll, müssen Sie den Registry Key

HKEY_LOCAL_MACHINE
SOFTWARE
Utimaco
Sgeasy
SgeLogoBackGnd

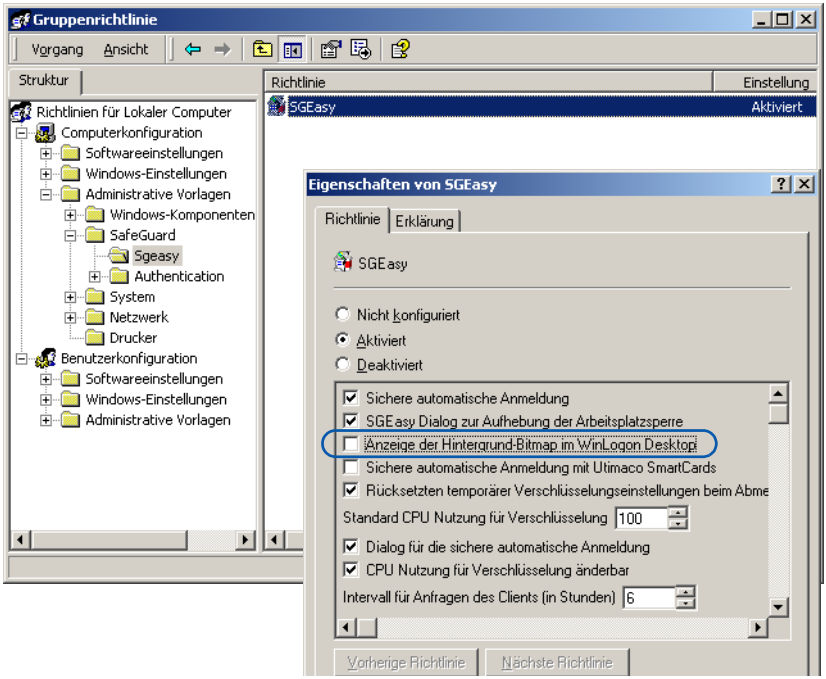
auf den Wert „0“ setzen.

Das Hintergrund-Bitmap kann auch über eine Richtlinie in Utimacos administrativer Vorlage ausgeblendet werden (siehe ’Häufig verwendete Registry-Einstellungen für SafeGuard Easy über die administrative Vorlage ändern’).

Die Richtlinie finden Sie unter

Computerkonfiguration
\Administrative Vorlagen
\SafeGuard
\Sgeasy

Unter „Eigenschaftenseite von SGEasy“ ist der Haken vor „**Anzeige der Hintergrund-Bitmap im WinLogon Desktop**“ zu entfernen. Daraufhin erscheint kein SafeGuard Easy-Bitmap mehr.



3.5 SafeGuard Easy auf einem PC mit mehreren Betriebssystemen installieren

SafeGuard Easy kann zum Schutz der Daten auf einem Rechner eingesetzt werden, wenn mehrere Betriebssysteme gleichzeitig in separaten Partitionen installiert sind. Damit die Betriebssysteme auch nach der SafeGuard Easy-Installation problemlos gestartet werden können, muss auf einem Betriebssystem die Kompletteinstallation von SafeGuard Easy, auf den anderen Betriebssystemen jeweils das sogenannte „**Laufzeitsystem**“ installiert werden.

Das Laufzeitsystem wird aus dem CD-Verzeichnis \RUNTIME gestartet (`Runtime.msi`). Ein Laufzeitsystem installiert zusätzlich das Programm zum Schalten der Disketten- und Geräteverschlüsselung (SGECRYPT).

So installieren Sie SafeGuard Easy auf einem PC mit mehreren Betriebssystemen:

1. Bestimmen Sie eine Windows-Installation zur primären Installation.
2. In der Folge booten Sie zunächst nacheinander alle nicht primären Windows-Installationen und installieren dort jeweils das Laufzeitsystem. Wählen Sie für jede Installation ein anderes Verzeichnis aus.
3. Abschließend müssen Sie Ihre primäre Windows-Installation booten, um dort SafeGuard Easy zu installieren.
4. Nach abgeschlossener Verschlüsselung können Sie dann auch alle nicht primären Windows-Installationen weiterhin booten.

4 Zentrale Installation

Administratoren können die gesamte Konfiguration der Benutzer-PCs im Vorfeld der zentralen Softwareverteilung festlegen.

Der Administrator erstellt für diesen Zweck an seinem PC eine Datei, die alle notwendigen SafeGuard Easy-Einstellungen für die Benutzer-PCs enthält. Diese Datei nennt SafeGuard Easy „Konfigurationsdatei“. Mit Hilfe der Konfigurationsdatei wird SafeGuard Easy auf den Benutzer-PCs installiert. Nachträgliche Änderungen an der SafeGuard Easy-Konfiguration sind über weitere Konfigurationsdateien immer möglich.

SafeGuard Easy kann in einer Umgebung mit oder ohne Active Directory installiert werden.

4.1 Konfigurationsdatei erstellen

So erstellen Sie eine Konfigurationsdatei:

1. Starten Sie den **Konfigurationsdateiassistenten** über Programme / Utimaco / SafeGuard Easy / Konfigurationsdateiassistent.
2. Wählen Sie als Konfigurationsdateityp „Installieren“.
3. Definieren Sie auf den Verwaltungsseiten des Konfigurationsdateiassistenten die SafeGuard Easy-Einstellungen für die Benutzer-PCs.

Das Endergebnis ist eine Datei mit dem Standardnamen `Install.cfg`.

Die Datei `Install.cfg` ist verschlüsselt und enthält die Passwörter der Benutzer und die Schlüssel für Festplatten/Disketten/Wechselmedien.

Weitere Details siehe ’Konfigurationsdateiassistent’.

HINWEIS:
Konfigurationsdateien sollten, wie alle Elemente einer Systemadministration, vor unbefugtem Zugriff geschützt und z.B. Benutzern nicht zugänglich gemacht werden.

4.2 Zentrale Installation mit Active Directory

SafeGuard Easy wird auf Benutzer-PCs in einer Active Directory-Umgebung installiert, indem eine MSI-Datei (`Sgeasy.msi`) zur Softwareverteilungsfunktion eines Gruppenrichtlinienobjekts (GPO) hinzugefügt wird.

Zum Bearbeiten der MSI-Datei benötigen Sie einen zusätzlichen Editor (z.B. ORCA oder NetInstall).

HINWEIS:
ORCA ist Teil des Microsoft Platform Software Development Kit (PSDK). PSDK kann von der Microsoft-Webseite heruntergeladen werden.

4.2.1 Voraussetzungen

- Auf den Benutzer-PCs muss entweder Windows 2000 oder Windows XP installiert sein.
- Auf den Benutzer-PCs muss auf der Systempartition genügend Speicherplatz verfügbar sein.
- Alle zur Installation vorgesehenen Benutzer-PCs müssen vor einem Neustart in die Organisationseinheit verschoben werden, für welche die konfigurierte GPO (Gruppenrichtlinienobjekt) verwendet wird.
- Alle Benutzer-PCs müssen für die zentrale Softwareverteilung an die Directory-Domäne angebunden sein, und es muss ein Computerkonto für den Benutzer-PC eingerichtet und aktiv sein.

4.2.2 MSI-Pakete mit einem Editor bearbeiten

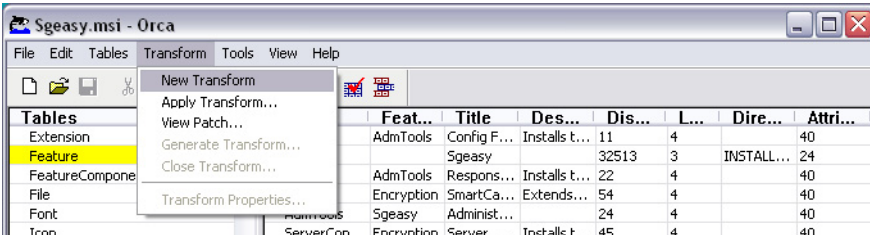
Im folgenden Abschnitt wird gezeigt, wie man mit dem Werkzeug *Orca* eine sogenannte Transform-Datei (Dateierweitertung .mst) erstellt, um Änderungen am MSI-Paket "Sgeasy.msi" vorzunehmen.

Eine MST-Dateien ändert die Installationseigenschaften der MSI-Datei, die MSI-Datei selbst bleibt im Urzustand.

> ***ACHTUNG:***
> Die Installation von modifizierten MSI-Paketen wird nicht unterstützt. Wir empfehlen die Verwendung von Transform-Dateien (MST) um Anpassungen vorzunehmen.

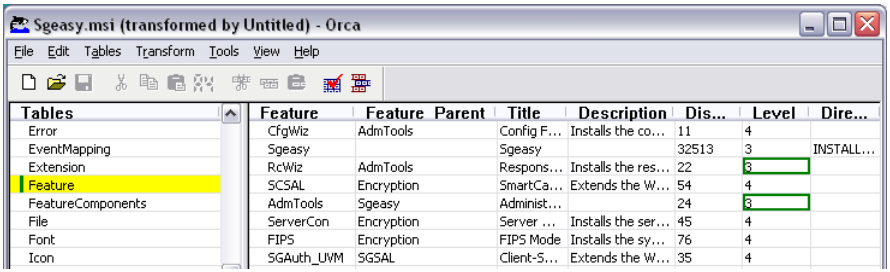
So erstellen Sie eine Transform-Datei:

1. Starten Sie Orca.msi.
2. Wählen Sie **File** > **Open** und öffnen Sie Sgeasy.msi.
3. Wählen Sie **Transform** > **New Transform**.



4. Wählen Sie unter **Tables** den Eintrag **Features** aus. Features sind alle SafeGuard Easy-Komponenten, die installiert werden sollen. Eine Beschreibung der einzelnen Features finden Sie unter 'SafeGuard Easy Funktionen'.

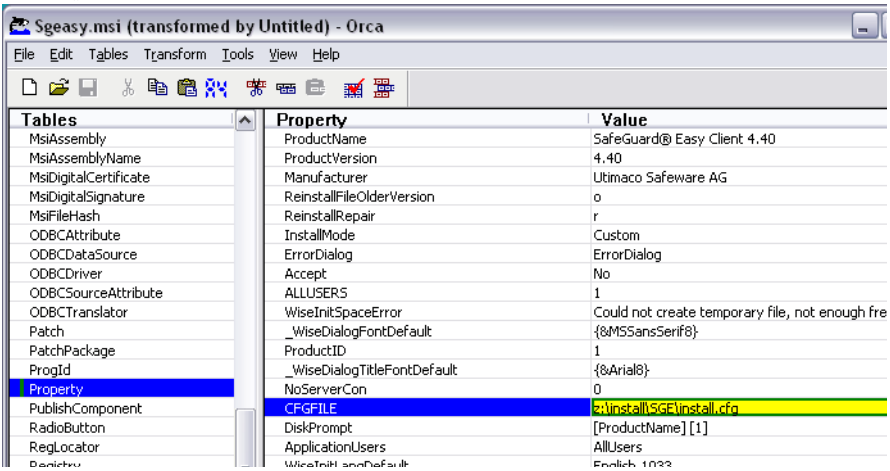
   Ob ein Feature installiert wird oder nicht, entscheidet der Wert in der Spalte „Level“:
   3 = Feature wird installiert
   4 = Feature wird nicht installiert


Sgeasy.msi (transformed by Untitled) - Orca
File Edit Tables Transform Tools View Help
Tables
Error
EventMapping
Extension
Feature
FeatureComponents
File
Font
Icon
Feature Feature_Parent Title Description Dis... Level Dire...
CfgWiz AdmTools Config F... Installs the co... 11 4
Sgeasy Sgeasy 32513 3 INSTALL...
RcWiz AdmTools Respons... Installs the res... 22 3
SCSAL Encryption SmartCa... Extends the W... 54 4
AdmTools Sgeasy Administ... 24 3
ServerCon Encryption Server ... Installs the ser... 45 4
FIPS Encryption FIPS Mode Installs the sy... 76 4
SGAuth_UWM SGSAL Client-S... Extends the W... 35 4

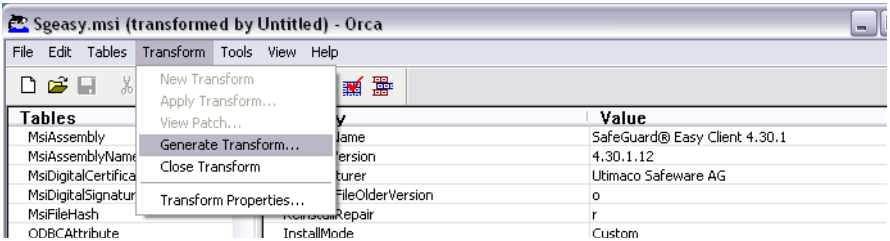
HINWEIS:
Wenn man ein Feature installieren will, muss man auch alle dazugehörigen "Feature Parents" (Vaterkomponenten) installieren!

5. Wählen Sie unter **Tables** den Eintrag **Property**. Es erscheinen alle alle Properties (= SafeGuard Easy Setup-Parameter). Eine Beschreibung der Parameter, die installiert werden dürfen, finden Sie unter 'SafeGuard Easy Parameter'.

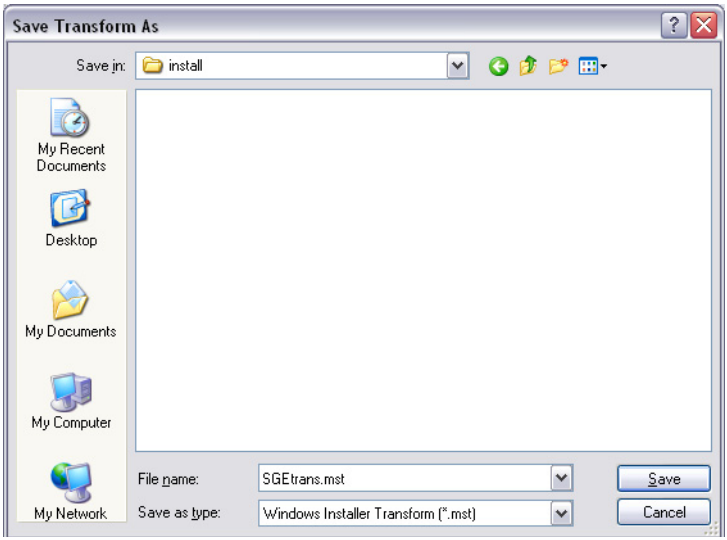
   Geben Sie z.B. den Namen und Ablageort der Konfigurationsdatei unter „CFGFILE“ an.



6. Wählen Sie **Transform** > **Generate Transform**.



7. Speichern Sie die Transform-Datei im freigegebenen Installationsverzeichnis (z.B. Z:/SGE/install).



8. Die Sgeasy.msi Datei kann nun unter Anwendung der Transform-Datei über msiexec.exe (siehe Beispiel) oder über eine entsprechende Gruppenrichtlinie (im AD) verteilt werden.

Beispiel für den Installationsaufruf:

msiexec /i sgeasy.msi /L*v c:\temp\easy.log TRANSFORMS=sgetrans.mst /qn

4.3 Zentrale Installation ohne Active Directory

Für die Installation von SafeGuard Easy ohne Active Directory-Umgebung benötigen Sie Softwareverteilungsprogramme von Drittanbietern.

Erstellen Sie zu diesem Zweck ein Installationspaket, das

- die SafeGuard Easy Programmdateien enthält
- ein Skript, das die Kommandozeile für die automatische Installation enthält.

Verteilen Sie das Installationspaket dann an die Clients.

4.3.1 Kommandozeile für automatische Installation

Wenn SafeGuard Easy ohne Active Directory installiert werden soll, ist das Programm „msiexec“ zu verwenden. „Msiexec“ ist in Windows 2000 und Windows XP bereits integriert und führt eine vorgefertigte SafeGuard Easy-Installation automatisch aus.

Da auch die Quelle und das Ziel für die Installation angegeben werden können, besteht die Möglichkeit zur einheitlichen Installation an mehreren PCs.

Kommandozeilensyntax

```
msiexec /i <Pfad+ Name der MSI-Datei> /qn ADDLOCAL=ALL |
<SGEasy Funktionen> <SGEasy Parameter+Konfigurationsdatei>
```

Die Kommandozeilensyntax setzt sich zusammen aus

- **Parametern des Windows Installer**, die z.B. Warnungen und Fehlermeldungen während der Installation in eine Datei protokollieren.
- **SafeGuard Easy Funktionen (Features)**, die mit einer MSI-Datei installiert werden sollen (z.B. SAL).
- **SafeGuard Easy Parametern**, über die z.B. Konfigurationsdateien mitgegeben werden.
- **einer Konfigurationsdatei**, für eine Installation mit der Eigenschaft „Installieren“.

BEISPIEL:

```
msiexec /i F:\Sgeasy.msi /qn /L* I:\Temp\SafeGuard
Easy.log ADDLOCAL=Sgeasy,Encryption,SGSAL In-
stalldir=C:\SafeGuard Easy CFGFILE=F:\Install.cfg
```

SafeGuard Easy wird mit Sicherem Automatischen Logon (SAL) im Verzeichnis C:\SafeGuard Easy installiert und im Verzeichnis I:\TEMP (muss existieren) wird die Protokolldatei SafeGuard Easy.log angelegt. Die vorkonfigurierten Einstellungen für SafeGuard Easy befinden sich in der Datei `Install.cfg`, die mit dem Konfigurationsdateiassistenten erzeugt wurde.

Die einzelnen Funktionen unter ADDLOCAL werden nur durch ein Komma und kein zusätzliches Leerzeichen getrennt. Achten Sie außerdem auf die Groß-/Kleinschreibung der einzelnen Funktionen und der SafeGuard Easy Parameter.

Wenn man eine Funktion auswählt, muss man auch alle Vaterkomponenten (Feature Parents) zur Kommandozeile hinzufügen!

4.3.2 Ausgewählte Optionen des Windows-Installers

> ***HINWEIS:***
> Alle verfügbaren Optionen können über „msiexec.exe“ in der Eingabeaufforderung abgerufen werden.

`/i`
Gibt an, dass es sich um eine Installation handelt.

`/qn`
Installiert ohne Benutzerinteraktion und zeigt keine Benutzeroberfläche an.

`ADDLOCAL=`
Listet die Funktionen (Features) auf, die installiert werden. Wird die Option nicht angegeben, werden alle Funktionen (Features) installiert, die für eine Standardinstallation vorgesehen sind.

`ALL`
Installiert alle verfügbaren Funktionen (Features).

`REBOOT=forcerestart | norestart`
Erzwingt oder unterdrückt Neustart nach Installation. Ohne Angabe wird der Neustart erzwungen (Force).

`/L*` <Pfad + Dateiname>
Protokolliert alle Warnungen und Fehlermeldungen in die angegebene Protokolldatei. Ausschließlich Fehlermeldungen protokolliert der Parameter `/Le <Pfad + Dateiname>`.

`Installdir=` <Verzeichnis>
Gibt das Verzeichnis an, in das SafeGuard Easy installiert wird.
Ohne Angabe wird als Standardinstallationsverzeichnis <SYSTEM>:\PROGRAMME\UTIMACO verwendet.

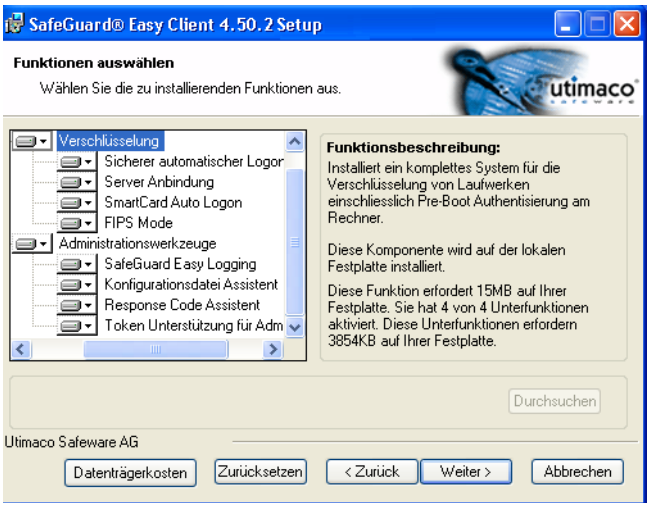
4.4 SafeGuard Easy Funktionen und Parameter

Für eine zentrale Installation muss bereits im Vorfeld definiert werden, welche SafeGuard Easy-Funktionen (Features)/-Parameter auf den Clients installiert werden. Bei einer Installation über Active Directory geschieht dies, indem die MSI-Datei mit einem Tool wie ORCA angepasst wird. Ohne Active Directory müssen die zu installierenden Funktionen (Features)/Parameter in eine Kommandozeilensyntax integriert werden.

4.4.1 SafeGuard Easy Funktionen

In den folgenden Tabellen sind alle Funktionen (Features) aufgelistet, die automatisch installiert werden können. Sie entsprechen zum Großteil denjenigen, die auch bei einer interaktiven Installation ausgewählt werden können.

Im Beispieldialog sehen Sie alle Funktionen (Features) von `Sgeasy.msi`, die bei einer angepassten, interaktiven Installation wählbar sind.



Installierbare Funktionen (Features) mit Sgeasy.msi		
Funktion (Feature)	**Vaterkomponente (Feature Parent)**	**Beschreibung**
Sgeasy	-----	Installiert alle notwendigen Dateien für SafeGuard Easy. Nach einem automatischen Neustart sind die Funktionen (Encryption, SGSAL usw.) nicht aktiv. Sie können nachträglich per Kommandozeile aktiviert werden oder manuell über Systemsteuerung / Programme hinzufügen/entfernen.
Encryption	Sgeasy	Installiert SafeGuard Easy inkl. SafeGuard Anmeldekomponente (Utimaco Master GINA)
FIPS	Encryption	Installiert den FIPS-Modus
SCSAL	Encryption	Installiert den SAL mit Smartcard
ServerCon	Encryption	Installiert die Server Anbindung (Netzwerkagenten) für die zentrale Administration
SGAuth_ MachineBinding	Encryption	Erweitert die Windows Anmeldeprozedur um die TPM Maschinenbindung Features
SGSAL	Encryption	Installiert den sicheren automatischen Logon (SAL)

Installierbare Funktionen (Features) mit Sgeasy.msi (Forts.)		
AdmTools	Sgeasy	Installiert die Administrationswerkzeuge (z.B. Konfigurationsdateiassistent, Response Code Assistent). Nach einem automatischen Neustart sind die Funktionen (Features) nicht aktiv. Sie können nachträglich ohne Benutzerinteraktion aktiviert werden oder manuell über Systemsteuerung / Programme hinzufügen/entfernen.
Auditing	AdmTools	Installiert die SafeGuard Easy Protokollierung
TokenSup	AdmTools	Installiert die Token-Anmeldung für die Administrationswerkzeuge
CfgWiz	AdmTools	Installiert den Konfigurationsdateiassistenten
RcWiz	AdmTools	Installiert den Response Code Assistenten
SGAuth_UVM	SGSAL	Erweitert die Windows Anmeldeprozedur um die Unterstützung der ThinkVantage „Client-Security-Integration“

Installierbare Funktionen (Features) mit Runtime.msi		
Parameter	**Vaterkomponente**	**Beschreibung**
`RuntimeSys`		Installiert ein Laufzeitsystem

Installierbare Funktionen (Features) mit Server.msi		
Funktion (Feature)	**Vaterkomponente (Feature Parent)**	**Beschreibung**
`Server`	---	Installiert den SafeGuard Easy Server inkl. Protokollierung
`SgeServer`	`Server`	Installiert den SafeGuard Easy Server
`RemAdmSupport`	`Server`	Installiert die Unterstützung für Remote Administration
`AdmConsole`	`Server`	Installiert die Administrationskonsole

4.4.2 SafeGuard Easy Parameter

> ***HINWEIS:***
> Alle Parameter in Großbuchstaben in die Kommandozeile eintragen!

`AUTOBACKUP=0|1`

Definiert, ob der Assistent für die Notfalldiskette zum Erzeugen einer Systemkernsicherung automatisch nach einer erfolgreichen Installation starten soll. In der Grundeinstellung startet AUTOBACKUP automatisch (AUTOBACKUP=1).

`CFGFILE=`<Konfigurations-/Migrationsdatei>

Definiert den kompletten Namen einer SafeGuard Easy Konfigurationsdatei für eine Installation/Migration.

`KERNELDRV=`<Name des Laufwerks (C,D,...)>

Definiert das Laufwerk, auf dem der SafeGuard Easy Systemkern gespeichert wird. In der Grundeinstellung ist es das Windows Bootlaufwerk. Ein Laufwerk zu bestimmen, auf dem der Systemkern gespeichert wird, ist beispielsweise dann hilfreich, wenn Sie die Windows Systempartition mit Tools wie GHOST wiederherstellen wollen. Das Wiederherstellen würde ansonsten den SafeGuard Easy Systemkern entfernen, da dieser in der Grundeinstellung immer auf der Systempartition abgelegt ist.

Das Ziellaufwerk muss auf der ersten Festplatte sein!

NOACTIVATION=0|1

Mit NoActivation=1 werden SafeGuard Easy-Dateien nur auf einen PC kopiert, das Programm aber nicht aktiviert. Nicht aktiviert heißt: Der Master Boot Record wird nicht ausgetauscht und der SafeGuard Easy Systemkern nicht installiert. Aktiviert wird SafeGuard Easy nachträglich per Konfigurationsdatei über das Kommando "execcfg"
(z.B. execcfg /f:C:\SGE\Install.cfg).

In der Grundeinstellung ist SafeGuard Easy aktiviert (NoActivation=0).

PARTCHECK=0|1

Überprüft, ob die vorhandenen Partitionstypen bekannte Dateisysteme unterstützen (FAT, FAT 32, NTFS,...). Wenn ein Partitionstyp unbekannt ist, wird die Installation abgebrochen. In der Grundeinstellung ist die Überprüfung aktiv (PARTCHECK=1).

SERVER=<Servername>

Definiert den Namen der Arbeitsstation, auf der der SafeGuard Easy Server installiert ist. Der Parameter kann nur verwendet werden, wenn die Komponente „Server Anbindung“ (unterstützt die zentrale Administration auf einem Client) für die Installation gewählt ist.

GROUPS=<Gruppenname1,Gruppenname2,...>

Definiert die (SafeGuard Easy) Gruppen, denen die Arbeitsstation im Rahmen der zentralen Administration zugeordnet wird, wenn sie sich am SafeGuard Easy Server registriert.Der Parameter kann nur verwendet werden, wenn die Komponente „Server Anbindung“ (unterstützt die zentrale Administration auf einem Client) gewählt ist.

`GINASYS=0|1`

Definiert, ob die SafeGuard Anmeldekomponente (Utimaco Master-GINA) zur Kontrolle der Windows Anmeldung installiert werden soll. In der Grundeinstellung wird die Utimaco Master-GINA installiert (GINASYS=1).

ACHTUNG:
Wir empfehlen Ihnen, die Utimaco Master-GINA immer einzusetzen. Das Utimaco GINA-System ist ein wichtiger funktioneller Bestandteil von SafeGuard Easy. Dem GINA-System wird in Zukunft immer größere Bedeutung zukommen, um neue Funktionalitäten zu implementieren. Ist die GINA nicht installiert, werden bestimmte Funktionalitäten nach der Migration zu der neuen Version nicht zur Verfügung stehen. Eine fehlende GINA kann sogar zukünftige Migrationen beeinträchtigen.

Ohne die Utimaco Master-GINA sind bestimmte Funktionen von SafeGuard Easy nach der Installation nicht verfügbar:

- Dialog für Verschlüsselung/Entschlüsselung wird nicht angezeigt, wenn der Benutzer nicht angemeldet ist
- Sicherer automatischer Logon und Automatische Smartcard-Anmeldung funktionieren nicht.
- Windows-Anmeldung wird bei aktivem Sicheren Wake On LAN nicht blockiert.
- Passwortsynchronisierung zwischen Windows und SafeGuard Easy funktioniert nicht.

5 Update

Haben Sie bereits eine Vorgängerversion von SafeGuard Easy auf Ihrer Arbeitsstation installiert, können Sie bequem einen Versionswechsel durchführen. Bereits getroffene Einstellungen (Benutzername, Benutzerpasswort etc.) bleiben erhalten.

Ein Update ist ab Version 4.11 (Buildnummer 4.11.0.138) möglich.

Ein Update wird entweder während der Installation der neuen Version gestartet oder automatisch mit Hilfe einer vorkonfigurierten Migrationsdatei durchgeführt. In beiden Fällen kommt der Migrationsassistent zum Einsatz.

5.1 Lokales Update

So führen Sie ein Update durch:

1. Auf der SafeGuard Easy-CD in das Verzeichnis \CLIENT wechseln und das Setup starten.
2. SafeGuard Easy entdeckt, dass bereits eine ältere Version auf einer Arbeitsstation installiert ist und zeigt dies in einem Dialog an.

SafeGuard Easy Setup
Willkommen beim SafeGuard® Easy Installationsassistenten
Eine ältere Version von SafeGuard Easy ist bereits installiert. Die Installation wird ein Upgrade durchführen.

3. Ein Prüfprogramm analysiert die Konsistenz des Systemkerns.

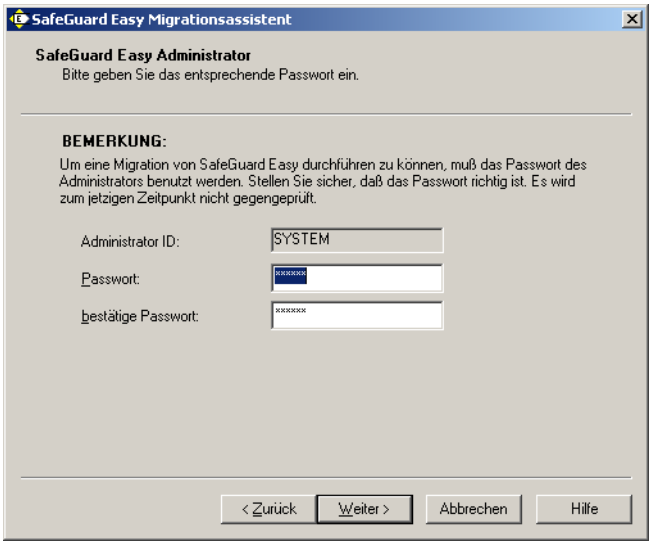
SafeGuard Easy Setup
Willkommen beim SafeGuard® Easy Installationsassistenten
Das Dateisystem wird analysiert. Bitte warten...

4. Ist der Systemkern in Ordnung, verläuft das Update problemlos und der Willkommen-Bildschirm erscheint.

   Ist der Systemkern nicht in Ordnung, muss er repariert werden.

5. Nacheinander Lizenzbedingungen akzeptieren, Zielverzeichnis für SafeGuard Easy bestimmen und Funktionen auswählen (SAL, Server Anbindung etc.).
6. Die SafeGuard Easy-Aktualisierung startet.
7. Der Dialog „SafeGuard Easy Administrator“ erscheint.

   Nur der SafeGuard Easy-Benutzer SYSTEM darf eine Migration auf einer Arbeitsstation ausführen. Zur Authentisierung muss hier das entsprechende SafeGuard Easy-Passwort eingetragen werden.


SafeGuard Easy Migrationsassistent
SafeGuard Easy Administrator
Bitte geben Sie das entsprechende Passwort ein.
BEMERKUNG:
Um eine Migration von SafeGuard Easy durchführen zu können, muß das Passwort des Administrators benutzt werden. Stellen Sie sicher, daß das Passwort richtig ist. Es wird zum jetzigen Zeitpunkt nicht gegengeprüft.
Administrator ID:
SYSTEM
Passwort:
bestätige Passwort:
< Zurück
Weiter >
Abbrechen
Hilfe

8. Der Dialog „Benutzung eines Tokens für eine Anmeldung“ erscheint.

   In den Versionen kleiner SafeGuard Easy 4.0 wurde keine Token-Unterstützung angeboten. Hier können Sie diese Ergänzung im Rahmen des Updates nachträglich vornehmen.

SafeGuard Easy Migrationsassistent
Benutzung eines Tokens für eine Anmeldung
Legen Sie fest, ob beim einer Anmeldung immer ein Token erforderlich ist oder dies vom anzumeldenden Benutzer abhängen soll.
Token für Anmeldung benutzen
Token für Anmeldung erforderlich
Ein Token ist immer erforderlich
Verwendung eines Tokens ist abhängig vom anzumeldenden Benutzer
Token Austellungmode bei Anmeldung
Ausstellung immer erlaubt
< Zurück
Weiter >
Abbrechen
Hilfe

- **Token für Anmeldung benutzen**
  Legt fest, ob die Token-Unterstützung aktiviert wird oder nicht.

- **Token für Anmeldung erforderlich**
  Bestimmt, ob sich alle SafeGuard Easy-Benutzer mit Token anmelden müssen oder nur ausgewählte Benutzer.

  – *Token ist immer erforderlich*
    Diese Option bedeutet, dass SafeGuard Easy die Token-Anmeldung für alle SafeGuard Easy Benutzer einer Arbeitsstation erzwingt.

    HINWEIS: Beim Verlust des Token ist keine temporäre Anmeldung per Challenge/Response möglich.

  – *Verwendung eines Token ist abhängig vom anzumeldenden Benutzer*
    Diese Option erlaubt größtmögliche Flexibilität, da einem SafeGuard Easy-Benutzer je nach Bedarf die Tokennutzung gewährt bzw. wieder entzogen werden kann (auch nach der Installation von SafeGuard Easy!).

- **Token-Ausstellungsmodus bei Anmeldung**
  Legt fest, wer berechtigt ist, SafeGuard Easy-Zugangsdaten auf einen Token zu schreiben.

  – *Ausstellung immer erlaubt:*
    SafeGuard Easy Benutzer darf den Token immer ausstellen.

  – *Externe Erlaubnis erforderlich:*
    Helpdesk ist involviert in Ausstellungsprozess (Challenge/Response-Verfahren).

  – *Keine Ausstellung durch den SGE Nutzer erlaubt:*
    SafeGuard Easy Benutzer darf keine Daten auf den Token schreiben, das Ausstellen übernimmt der Helpdesk (Token Administration).

Nähere Informationen siehe 'Token-Unterstützung'.

9. Der Dialog „Zielverzeichnis“ für Migrationsdatei erscheint.

   Legen Sie fest, in welchem Pfad Sie die Migrationsdatei `Sgemig.cfg` speichern wollen. Die Migrationsdatei enthält das SYSTEM-Passwort und die Einstellungen für die Token-Unterstützung. Das Programm erkennt, in welchem Verzeichnis die bisherige SafeGuard Easy-Version abgelegt war und stellt diesen Pfad als Vorgabe ein. Wenn Sie auf die [Durchsuchen]-Schaltfläche klicken, können Sie selbst entscheiden, in welchem Laufwerk und in welchem Verzeichnis die Datei abgelegt werden soll.

   Klicken Sie auf [Weiter], wird die Migrationsdatei erstellt und die Migration gestartet.

5.2 Update mit Migrationsdatei

Für ein automatisiertes Update muss mit dem Migrationsassistenten der neuesten SafeGuard Easy-Programmversion eine Migrationsdatei erstellt werden. Diese Migrationsdatei wird dann über msiexec ausgeführt.

Migrationsdatei erstellen

So erstellen Sie eine Migrationsdatei:

1. Installieren Sie auf einem Administrator-PC mindestens den Konfigurationsdateiassistenten. Danach ist auch der Migrationsassistent verfügbar.
2. Starten Sie den Migrationsassistenten über WIZLDR.exe im SafeGuard Easy-Verzeichnis.
3. Machen Sie im Migrationsassistenten alle notwendigen Angaben (siehe 'Lokales Update').
4. Die Datei SGEMig.cfg wird im gewählten Verzeichnis angelegt.

Beispiel für Kommandozeile

```
msiexec /i D:\Sgeasy.msi CFGFILE=D:\SGEmig.cfg /qn
```

Spezialfall: Zentrale Administration
Wenn ein SafeGuard Easy Client nach dem Update über die SafeGuard Easy Administrationskonsole zentral administriert werden soll, vergessen Sie nicht, die entsprechenden Funktionen (ServerCon) und Parameter (SERVER) in die Kommandozeile mit aufzunehmen, z. B.:

```
msiexec /i D:\Sgeasy.msi ADDLOCAL=Sgeasy,Encryption,ServerCon
CFGFILE=D:\SGEmig.cfg SERVER=Server01 /qn
```

HINWEIS:
Die Serveranbindung kann nach dem Update nicht mehr nachträglich aktiviert werden, sondern erfordert eine Neuinstallation von SafeGuard Easy.

Nach dem Update

Nach dem Update erfolgt ein Neustart und die Migration ist abgeschlossen.

5.3 Systemkern-Prüfung beim Update

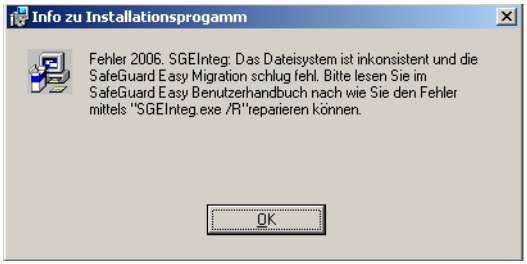
Für ein erfolgreiches Update muss der SafeGuard Easy-Systemkern intakt sein. Ab Version 4.20.1 prüft SafeGuard Easy dies vor jedem Update, und der Benutzer erhält einen Hinweis im Setup-Dialog („Ihr Dateisystem wird gerade analysiert, bitte warten Sie...“).

Ist der Systemkern in Ordnung, verläuft das Update problemlos.

Ist der Systemkern nicht in Ordnung, erscheint am Bildschirm eine Fehlermeldung, die auf mögliche Probleme hinweist und das Ausführen eines Reparaturprogramms (SGEInteg) vor dem Update empfiehlt.

5.3.1 Was passiert, wenn der Systemkern nicht in Ordnung ist

1. SafeGuard Easy-Update starten.
2. Das Prüfprogramm SGEInteg startet im Hintergrund, analysiert den Systemkern und stellt fest, dass dieser nicht in Ordnung ist.
3. Es erscheint eine Dialog-Meldung („SGEInteg: Das Dateisystem ist inkonsistent. Die SafeGuard Easy-Migration schlug fehl. Bitte lesen Sie im SafeGuard Easy-Benutzerhandbuch nach, wie Sie den Fehler mittels SGEInteg /R reparieren können.“).


Info zu Installationsprogamm
Fehler 2006. SGEInteg: Das Dateisystem ist inkonsistent und die SafeGuard Easy Migration schlug fehl. Bitte lesen Sie im SafeGuard Easy Benutzerhandbuch nach wie Sie den Fehler mittels "SGEInteg.exe /R" reparieren können.
OK

Das Setup bricht an dieser Stelle ab. Bei einer automatischen Installation wird die Fehlernummer „2006“ in die Windows Installer Protokolldatei geschrieben (Protokollierung muss eingeschaltet sein).

4. Über die Kommandozeile „SGEInteg /R“ aufrufen. SGEInteg befindet sich auf der SafeGuard Easy-CD im Verzeichnis \Tools.

   SGEInteg repariert Dateien und Dateisystem in zwei Stufen: Zunächst werden alle Dateifehler korrigiert, die keinen Neustart verlangen. Werden Dateifehler mit Neustart-Forderung entdeckt, stößt SGEInteg die Überprüfung der Festplatte (Chkdsk) an. Stimmt der Benutzer einem Neustart des Rechners zu, wird Chkdsk ausgeführt.

5.3.2 Über das Reparaturprogramm

Das Reparaturprogramm SGEInteg startet automatisch beim Update zur aktuellen SafeGuard Easy-Version. Der Benutzer/Administrator kann es auch manuell (z. B. mit einem zusätzlichen Parameter) aus dem Tools-Verzeichnis der CD aufrufen.

SGEInteg repariert beim Aufruf mit Parameter /R das Dateisystem. SGEInteg meldet sowohl reparierbare als auch fatale Fehler. Bei der Reparatur ist es vielleicht notwendig, anschließend das Programm zur Überprüfung der Festplatte (chkdsk) zu starten. In der Regel startet der Rechner dann nochmal neu.

5.3.3 Parameter für das Reparaturprogramm

SGEInteg kann mit folgenden Parametern aufgerufen werden:

```
SGEINTEG [/?] [/c] [/r] [/p] [/d] [/len] [/v] [/y]
```

/?	Hilfe Zeigt alle Parameter an.
/c	Startet die Analyse des Dateisystems
/r	Aktiviert den Reparatur-Modus Identifizierte Dateisystem-Fehler werden repariert. Ruft man 'SGEInteg /R' auf, so wird auch der Parameter '/P' und eine Dateisystemanalyse durchgeführt. Dies kann allerdings einen Reboot nach sich ziehen.
/p	Korrigiert die SafeGuard Easy-Pfadangabe unter HKEY_LOCAL_MACHINE SOFTWARE Microsoft Windows CurrentVersion Run Ältere Versionen von SafeGuard Easy fügen in diesen Registrierungseintrag Pfadangaben ohne Anführungszeichen ein. Bei neueren Windows-Versionen führt dies unter Umständen dazu, dass diese Programme nicht ausgeführt werden. Mit diesem Parameter korrigiert SGEInteg die Pfadangaben. Der Rechner muss anschließend neu gestartet werden. Ruft man 'SGEInteg' ohne Parameter auf, so wird die Pfadangabe korrigiert und eine Dateisystemanalyse durchgeführt.

/d	Stellt den CRAREA Registrierungseintrag wieder her Ältere Versionen von SafeGuard Easy hatten Probleme, diesen Registrierungseintrag während der Installation zu erzeugen. Wenn der Registrierungseintrag nicht vorhanden ist, kann es zu Problemen bei Deinstallation und Update zu neuen Versionen kommen. SGEInteg /d stellt den Eintrag wieder her unter HKEY_LOCAL_MACHINE SOFTWARE Utimaco SGEasy CRAREA
/len	Behebt ein Problem mit Rescue and Recovery (RnR) Beim Update zur aktuellen SafeGuard Easy-Version kann bei installiertem RnR folgendes Problem auftreten: Das Programm 'SGEDemon.exe' erscheint nach jedem Neustart und bricht anschließend wieder ab. Da 'SGEDemon' nach dem Update nur einmal zur Anzeige einer Warnmeldung nötig ist, kann es ohne negative Folgen deaktiviert werden. SGEInteg /len entfernt 'SGEDemon.exe' aus HKEY_LOCAL_MACHINE SOFTWARE Microsoft Windows CurrentVersion Run
/v	Aktiviert Verbose Modus Der Verbose-Modus gibt ausführlichere Status-/ Fehlermeldungen auf dem Bildschirm aus.
/y	Aktiviert unbeaufsichtigten Modus Alle Dialoge werden automatisch mit JA bestätigt.

6 Deinstallation

Eine Deinstallation von SafeGuard Easy zieht folgende Wirkungen nach sich:

- Alle bislang verschlüsselten Bereiche der Festplatte(n) werden entschlüsselt.
- Die Pre-Boot Authentisierung wird - wenn installiert - entfernt.
- Die ursprüngliche Windows-Anmeldung wird wieder hergestellt, wenn SAL/Smartcard-SAL installiert war.
- Alle SafeGuard Easy-Dateien werden gelöscht.
- Alle Registrierungseinträge von SafeGuard Easy werden entfernt.

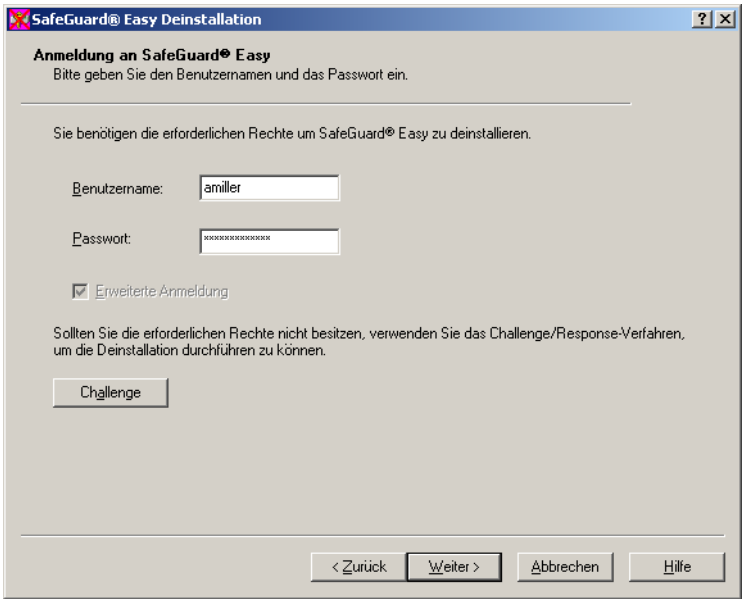
In der Grundeinstellung kann SafeGuard Easy nur vom Benutzer SYSTEM deinstalliert werden. Generell darf aber jeder SafeGuard Easy Benutzer das Programm von einer Arbeitsstation entfernen, der das Recht zur Deinstallation besitzt.

HINWEIS:
Versuchen Sie nicht, SafeGuard Easy durch Löschen der Dateien zu entfernen. Wird SafeGuard Easy nicht korrekt deinstalliert, bleiben Einträge in der Registrierungsdatenbank bestehen. Eine nochmalige Installation von SafeGuard Easy könnte deswegen möglicherweise fehl schlagen. In diesem Fall sollten Sie das Betriebssystem des Rechners neu installieren.

6.1 Lokale Deinstallation

So deinstallieren Sie SafeGuard Easy:

1. Wählen Sie nacheinander Start / Programme / Einstellungen / Systemsteuerung / Software und dann den Eintrag „SafeGuard Easy“ (oder „Server“/„Runtime“).
2. Klicken Sie auf [Entfernen].
3. Klicken Sie auf [Weiter] im Willkommenbildschirm. Es erscheint der Dialog *Anmeldung an SafeGuard Easy*.


SafeGuard® Easy Deinstallation
Anmeldung an SafeGuard® Easy
Bitte geben Sie den Benutzernamen und das Passwort ein.
Sie benötigen die erforderlichen Rechte um SafeGuard® Easy zu deinstallieren.
Benutzername:
amiller
Passwort:
Erweiterte Anmeldung
Sollten Sie die erforderlichen Rechte nicht besitzen, verwenden Sie das Challenge/Response-Verfahren, um die Deinstallation durchführen zu können.
Challenge
< Zurück
Weiter >
Abbrechen
Hilfe

4. Geben Sie Benutzername und Passwort ein. Sie müssen das SafeGuard Easy-Recht „Deinstallieren“ besitzen.
5. Klicken Sie auf [Weiter], beginnt SafeGuard Easy nach dem Bestätigen der Sicherheitsabfrage automatisch mit der Deinstallation.

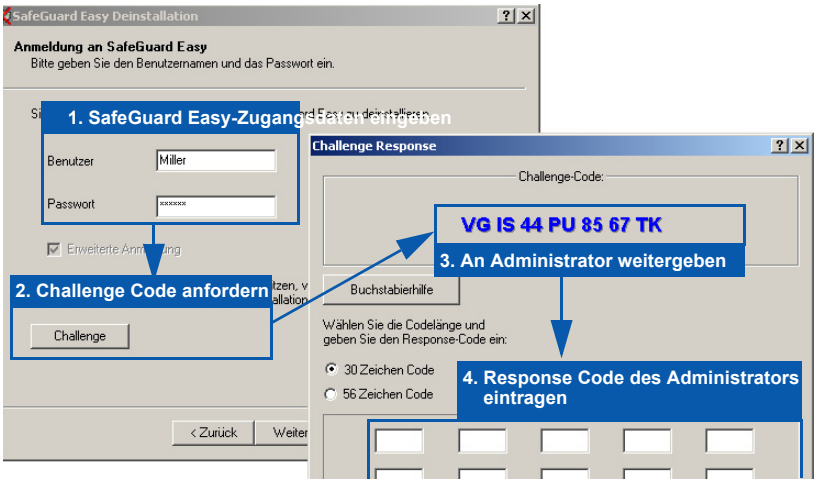
6.2 Deinstallation mit Challenge/ Response

Wenn ein SafeGuard Easy Benutzer laut seinem Benutzerprofil nicht zur Deinstallation von SafeGuard Easy berechtigt ist, kann ihm der Administrator dieses Recht mit Hilfe des Challenge/Response-Verfahrens gewähren. Zu diesem Zweck tauschen Benutzer und Administrator Challenge und Response Code aus.

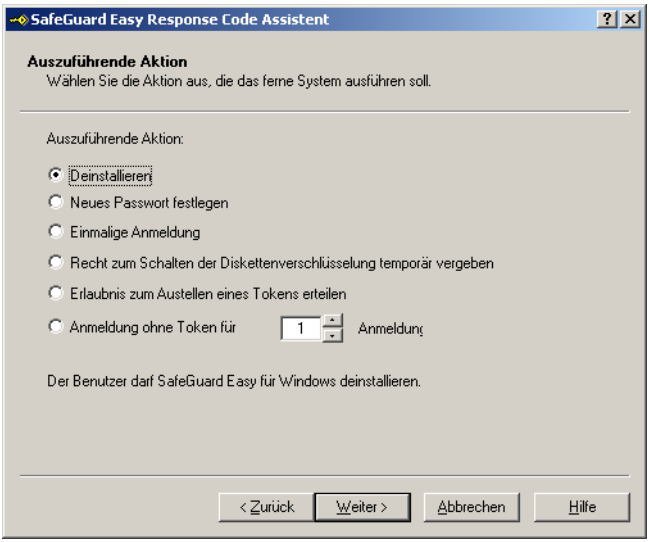
Der Erzeuger des Response Codes (Administrator) muss ein SafeGuard Easy Benutzerprofil auf dem Benutzer-PC kennen, das über das Recht zur Deinstallation verfügt. Zusätzlich muss dieses Benutzerprofil auf dem Benutzer-PC immer *wenigstens über die gleichen Rechte* wie der anfragende Benutzer verfügen.

So deinstallieren Sie SafeGuard Easy mit Challenge/Response:

1. Der Benutzer leitet die Deinstallation ein (siehe 'Lokale Deinstallation') und gelangt in den Dialog *Anmeldung an SG Easy*.
2. Der Benutzer gibt seine SafeGuard Easy-Zugangsdaten ein, fordert den Challenge Code an und gibt ihn per Telefon, SMS oder Mail an den Administrator weiter.



3. Der Administrator erzeugt mit dem Response Code Assistenten einen Response Code mit den SafeGuard Easy-Zugangsdaten des Benutzers (im Beispiel Benutzer „Miller“). Dem Response Code wird das Recht zur Deinstallation mitgegeben.



4. Nach Austausch von Challenge und Response Code wird SafeGuard Easy deinstalliert.

6.3 Vorkonfigurierte Deinstallation mit Konfigurationsdatei

Die Deinstallation von SafeGuard Easy läuft automatisiert ab, wenn eine Konfigurationsdatei mit der Eigenschaft „Deinstallieren“ über das Kommando "msiexec" aufgerufen wird.

Kommandozeilensyntax

```
msiexec /x D:\Sgeasy.msi CFGFILE=D:\Deinstall.cfg /qn
```

7 Systemstart und Anmeldung

SafeGuard Easy schaltet vor die Windows-Anmeldung einen eigenen Authentisierungsmechanismus vor den Bootprozess, die sogenannte Pre-Boot Authentisierung. Die Anmeldung an der Pre-Boot Authentisierung ist die voreingestellte Methode nach der Installation.

Wenn die Pre-Boot Authentisierung eingeschaltet ist, kann sich der Benutzer nur mit SafeGuard Easy-Zugangsdaten anmelden. Aus dem eingegebenen Passwort wird der zum Booten erforderliche Schlüssel berechnet, der eine verschlüsselten Festplatte entschlüsselt.

Wenn die Pre-Boot Authentisierung ausgeschaltet ist, bleibt die Festplatte verschlüsselt. Der PC bootet aber ohne Benutzerinteraktion bis zum Windows-Anmeldebildschirm. In diesem Fall werden Pre-Boot (SafeGuard Easy)-Daten versteckt auf der Festplatte gespeichert. Ohne Pre-Boot Authentisierung ist das Sicherheitsniveau eines Systems niedriger als mit Pre-Boot Authentisierung.

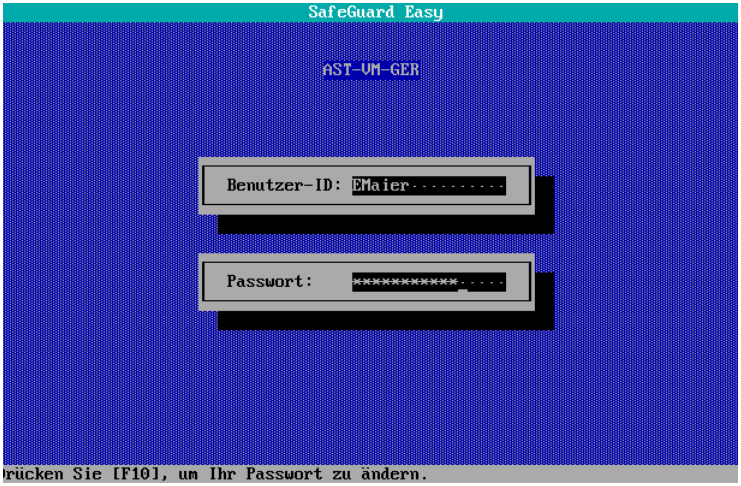
Benutzer können sich in der Pre-Boot Authentisierung anmelden

- als regulärer Benutzer (mit Benutzername und Passwort)
- als Standard-Benutzer (nur mit Passwort)
- mit Token (mit Token-Passwort)

Der Anmeldebildschirm der Pre-Boot Authentisierung hat folgende Merkmale und Funktionen:

- Name der Arbeitsstation und Text für rechtliche Hinweise
- Hilfe-Funktion zum Ändern des SafeGuard Easy/Token Passworts
- Hilfe-Funktion zum Zurücksetzen vergessener Passwörter

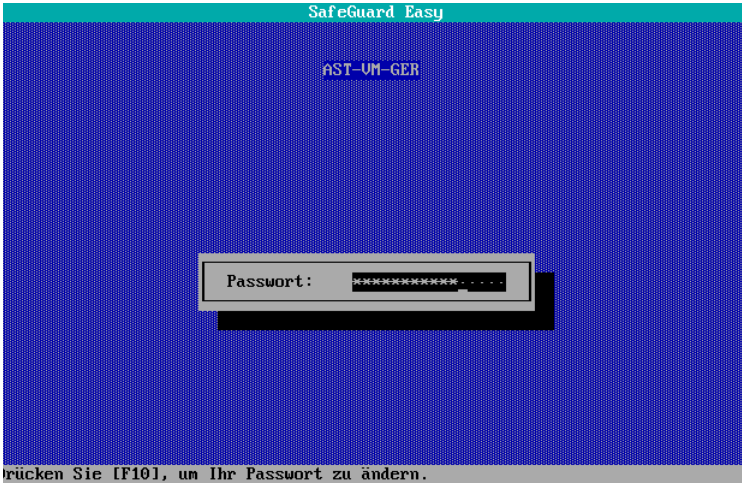
7.1 Als regulärer Benutzer anmelden



Im Normalfall melden sich Benutzer an der Pre-Boot Authentisierung mit ihrem SafeGuard Easy-Benutzernamen und -Passwort an.

Unter dem Produktnamen wird der Name der Arbeitsstation angezeigt (im Beispiel „AST-VM-GER“). Diese Daten werden aus den Systemeinstellungen Ihrer Arbeitsstation übernommen.

7.2 Als Standardbenutzer anmelden



Ist auf einer Arbeitsstation ein beliebiger SafeGuard Easy-Benutzer als „Standardbenutzer“ festgelegt, wird immer nur das SafeGuard Easy Passwort abgefragt. Die zusätzliche Eingabe des Benutzernamens entfällt.

7.2.1 Erweiterte Anmeldung über die Taste [F2]

Will sich jemand anderer als der Standardbenutzer anmelden, muss die *erweiterte Anmeldung* eingeschaltet werden, d.h. zusätzlich zum SafeGuard Easy-Passwort auch der Benutzername eingetragen werden.

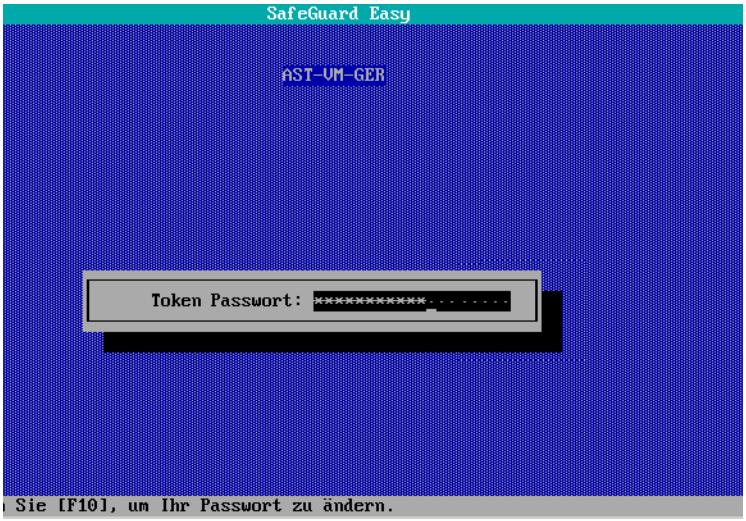
Wird [F2] gedrückt, erscheint über der Abfragezeile für das Passwort das Feld für die Eingabe des Benutzernamens.

ACHTUNG:
Der Benutzer SYSTEM muss sich **immer** mit Benutzernamen und Passwort anmelden.

7.3 Mit Token anmelden

SafeGuard Easy gibt Ihnen die Möglichkeit, sich mit einem Token an der Pre-Boot Authentisierung anzumelden. Dies stellt einen schnellen und bequemen Weg dar, sich an Ihren abgesicherten PC anzumelden.

Ist ein USB-Token gesteckt, enthält der Pre-Boot Authentisierung-Dialog ein Eingabefeld für das Passwort Ihres Token. Nach Bestätigen der Eingabe wird verglichen, ob der auf dem Token gespeicherte SafeGuard Easy Benutzer auf dem PC vorhanden ist. Bei Übereinstimmung der Daten wird die Anmeldung durchgeführt.

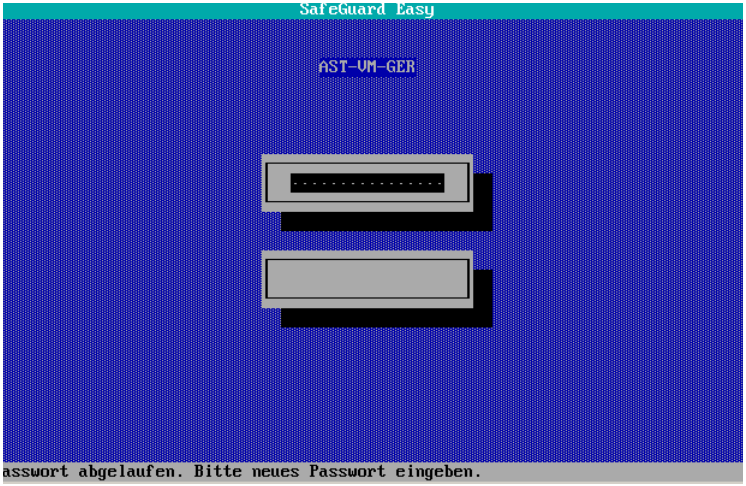


7.4 SafeGuard Easy-Passwort über die Taste [F10] ändern

Benutzer können das SafeGuard Easy Passwort über die Taste [F10] selbständig ändern. Der Benutzer gibt in diesem Fall zunächst seine aktuellen SafeGuard Easy-Zugangsdaten ein und bestätigt die Einträge mit [F10]. Anschließend erscheint die Aufforderung, ein neues Passwort einzugeben.

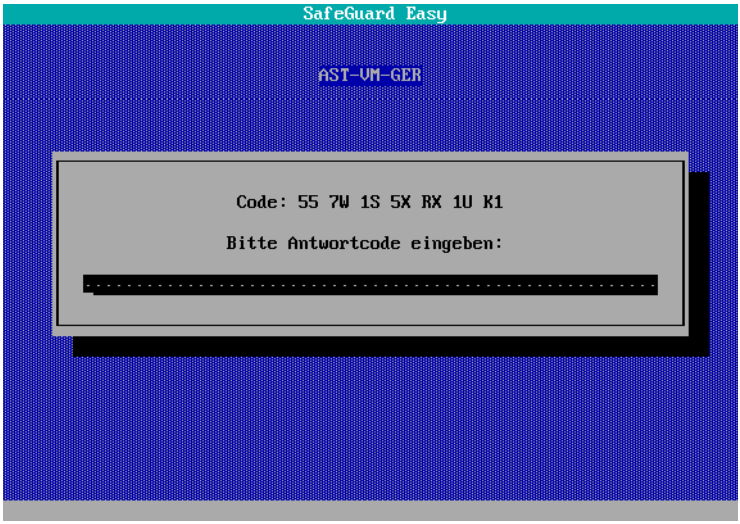
Der SafeGuard Easy Administrator kann Benutzern aber auch vorschreiben, nach Ablauf einer gewissen Zeitspanne ein neues Passwort zu definieren.

Bei einer Anmeldung mit Token dient [F10] dazu, das Token-Passwort zu ändern und nicht die SafeGuard Easy-Zugangsdaten auf dem Token.



7.5 Vergessene Passwörter über die Taste [F9] zurücksetzen

SafeGuard Easy bietet ein Challenge/Response-Verfahren zum Zurücksetzen „vergessener“ Passworts. Benötigt ein Benutzer Hilfe, muss er in der Pre-Boot Authentisierung durch Drücken der Taste [F9] einen Challenge Code erzeugen.



Dieser Challenge Code wird auf dem Bildschirm des Benutzers als ASCII Zeichenkette (14 Zeichen) angezeigt. Der Benutzer ruft anschließend bei seinem Administrator an und gibt seine Benutzerinformationen und den Challenge Code an. Der Administrator erzeugt dann einen Response Code. Nach der Eingabe dieses Response Codes auf dem Benutzer-PC, kann der Benutzer sein Passwort neu setzen.

Details zum Challenge/Response-Verfahren lesen Sie bitte im Kapitel ’Fernwartung (Challenge/Response)’ nach.

7.6 Fehlgeschlagene Anmeldung

Die Anmeldung in der Pre-Boot Authentisierung schlägt fehl, wenn

- der SafeGuard Easy-Benutzername falsch eingegeben wird.
- das SafeGuard Easy-Passwort nicht korrekt ist.
- das Token-Passwort nicht korrekt ist.
- das SafeGuard Easy Benutzerprofil abgelaufen ist (siehe Ablaufdatum').

Hat ein Benutzer seine SafeGuard Easy-Benutzerdaten falsch eingegeben, muss er einige Sekunden warten, bis er sich erneut anmelden kann. Aus Sicherheitsgründen erhöht sich die Wartezeit ab dem zweiten Fehlversuch. Durch eine einmalige korrekte Anmeldung wird die Wartezeit zurückgesetzt.

Fehlgeschlagene Anmeldung zurücksetzen

Sie können eine fehlgeschlagene Anmeldung folgendermaßen zurücksetzen:

1. Legen Sie die Notfalldiskette ein und booten Sie von Laufwerk A.
2. Rufen Sie das Programm Sgeasy.exe auf und geben Sie die korrekten SafeGuard Easy-Zugangsdaten ein.
3. Ein Menü mit Deinstallieren, Restaurieren und Reparieren erscheint. Verlassen Sie das Menü mit einem Klick auf [Abbrechen].

Starten Sie das System neu, wird die Wartezeit zurückgesetzt.

7.7 Anmeldung mit Pre-Boot Authentisierung über die Taste [F2] erzwingen

Bei ausgeschalteter Pre-Boot Authentisierung ist es möglich, nach Erscheinen eines Disketten-Symbols in der linken, oberen Monitorecke über [F2] den Pre-Boot Authentisierung-Anmeldedialog aufzurufen und sich wie gewohnt anzumelden.

7.8 Automatische Anmeldung an das Betriebssystem

SafeGuard Easy kann optional eine automatische Anmeldung an Windows durchführen. Diese Funktion nennt SafeGuard Easy *Sicherer Automatischer Logon* (kurz SAL). Der SAL legt die Windows-Daten nach einmaliger Eingabe in einem geschützten Bereich ab und greift nach jeder erfolgreichen Benutzer-Anmeldung in der Pre-Boot Authentisierung darauf zurück.

Einzige Voraussetzung für den SAL ist, dass die Pre-Boot Authentisierung eingeschaltet sein muss.

Der SAL-Dialog erscheint nach der Anmeldung an das Betriebssystem.

SafeGuard Easy - Sicherer Automatischer Logon
SafeGuard Easy kann Sie mit den gerade gemachten Angaben automatisch an Windows anmelden, wann immer Sie sich beim Systemstart mit dem derzeitigen SafeGuard Easy Benutzer anmelden.
Wollen Sie in Zukunft automatisch an Windows angemeldet werden ?
Diesen Dialog für den angemeldeten SafeGuard Easy Benutzer nicht mehr anzeigen
Ja
Nein

Wird die Frage nach der automatischen Anmeldung bejaht, sind in Zukunft nur noch die SafeGuard Easy-Zugangsdaten zur Anmeldung nötig.

Der SAL kann auch in Verbindung mit Smartcards eingesetzt werden.

Details zur automatischen Anmeldung lesen Sie bitte im Kapitel Windows-Anmeldung konfigurieren' nach.

7.9 Kompatibilität mit Anmeldekomponenten anderer Hersteller

Um die Sicherheit immer zu gewährleisten, stellen die Anmeldekomponenten von Utimaco sicher, dass sie immer zuerst vom Betriebssystem aufgerufen werden. Eine Änderung dieser Aufrufsequenz (z.B. durch Installation fremder Anmeldesoftware) wird automatisch wieder rückgängig gemacht.

Sollte dies bei einem nachfolgenden Reboot dazu führen, dass Sie sich nicht mehr an Windows anmelden können oder Windows nach der Anmeldung nicht ordnungsgemäß zur Verfügung steht, bietet Utimaco dem Administrator zwei Möglichkeiten, diese automatische Änderung aufzuheben:

- Wird während des Bootvorgangs nach Umschalten des blauen Bildschirms auf den Desktop [F8] gedrückt, startet das Betriebssystem weiter, und der Administrator erhält die Möglichkeit, manuell die von Utimaco aufgerufene zusätzliche Anmeldekomponente zu definieren.

- Wird [F8] nicht gedrückt, erscheint eine Abfrage, die es einem Anwender zu entscheiden erlaubt, ob die original Microsoft Anmeldekomponente oder die eines Drittherstellers nach Aufruf der Utimaco Anmeldekomponente angesprochen werden soll. Diese Abfrage erscheint solange, bis der Anwender zusätzlich entscheidet, die Abfrage zu deaktivieren. In diesem Fall bleibt die letzte getroffene Auswahl gültig. Die Verwendung der original Microsoft Komponente stellt ein korrektes Funktionieren des Logon sicher, deaktiviert aber gegebenenfalls einige Funktionen des zusätzlichen Drittherstellerprodukts. Mangels geeigneter Standardisierung ist es nicht in allen Fällen möglich, beliebige Windows Anmeldeprodukte gleichzeitig auf einer Maschine zu betreiben.

Im Fall umfangreicher „Rollouts“, besteht die Möglichkeit, dieses Programmverhalten vorab zu konfigurieren.
Zu diesem Zweck muss unmittelbar nach der Installation neuer Software und vor dem nachfolgenden Systemstart sichergestellt sein, dass der Registry-Eintrag „ForceKnownGina“ im Schlüssel „HKEY_LOCAL_MACHINE\Software\Utimaco\SGLogon“ von 0 auf 1 (neue Komponente wird durch Utimaco Anmeldekomponente aufgerufen) gesetzt wird. Durch das Setzen dieses Wertes auf 2 wird auch weiterhin die original Microsoft Anmeldekomponente von Utimaco aufgerufen.

8 Verwaltung im Überblick

SafeGuard Easy ist über das Konfigurationsprogramm (Konfigurationsdateiassistent) oder über die SafeGuard Easy Administration konfigurierbar. Über die Administration wird direkt in die SafeGuard Easy Konfiguration des PC eingegriffen, sie eignet sich für die lokale Verwaltung an einem einzelnen PC. Der Konfigurationsdateiassistent ändert nichts an den lokalen Einstellungen, sondern sammelt SafeGuard Easy-Einstellungen in einer Datei, die dann an Clients verteilt wird.

Die Verwaltungsprogramme unterscheiden sich in den möglichen Einstellungen nur geringfügig. In beiden Programmen ist es vorgeschrieben, sich mit korrekten SafeGuard Easy-Zugangsdaten zu authentisieren, um Veränderungen durchführen zu dürfen.

Welches der beiden Programme zu verwenden ist, hängt von Ihrer individuellen Situation ab, und wird im folgenden beschrieben.

8.1 Funktionstrennung

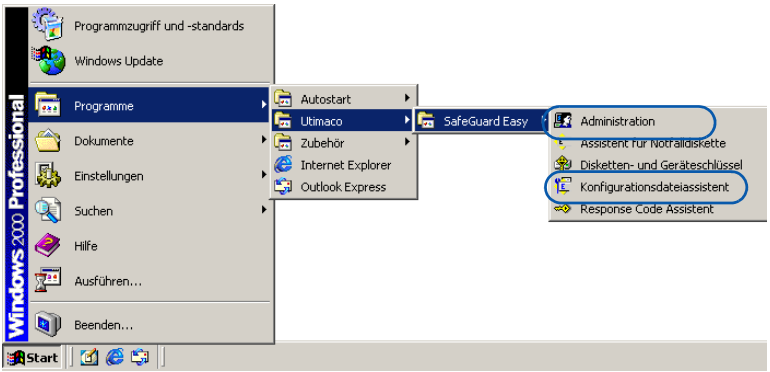
Zunächst muss definiert werden, ob die Funktion des Administrators mit der des „einfachen“ Benutzers kombiniert oder getrennt wird. Bei getrennten Funktionen besteht die Möglichkeit zusätzlich einen/mehrere Verwaltungsgehilfen mit einzubeziehen.

- **Kombinierte Funktion:** Der Benutzer ist selbst der Administrator. Er konfiguriert SafeGuard Easy an seinem PC für sich selbst (eine Person). Alle Einstellungen werden in der Administration vorgenommen. Das Konfigurationsprogramm wird nicht benötigt. Es muss auch keine Konfigurationsdatei erstellt werden.

- **Getrennte Funktionen an einem PC:** Der Administrator konfiguriert SafeGuard Easy am Benutzer-PC. Definiert er neben dem Benutzer auch einen Verwalter, haben drei Personen Zugriff. Es können beliebig viele Personen hinzugefügt werden, deren Rechte individuell einstellbar sind. Die Konfiguration erfolgt in der Administration. Das Konfigurationsprogramm wird nicht benötigt, da keine Konfigurationsdatei erstellt werden muss.

- **Getrennte Funktionen an mehreren PCs:** Der Administrator konfiguriert SafeGuard Easy an seinem PC für mehrere Arbeitsstationen. Für die weiteren Verwaltungsaufgaben kann ein Verwaltungsgehilfe eingebunden werden. Für diese Aufgabe verwenden Sie den Konfigurationsdateiassistenten. Damit erstellen Sie eine Datei, in der die Definitionen gesichert werden. Die Konfigurationsdatei wird über eine vorkonfigurierte Installation an die Benutzer-PCs weitergegeben. Wenn Sie am Administrator-PC andere Einstellungen verwenden wollen, ist auch die Administration zu verwenden.

8.2 Administration und Konfigurationsdateiassistenten starten



Nach einer Komplettinstallation legt SafeGuard Easy einen gleichnamigen Ordner unter Programme / Utimaco an. Über diesen sind die Administration und der Konfigurationsdateiassistent startbar.

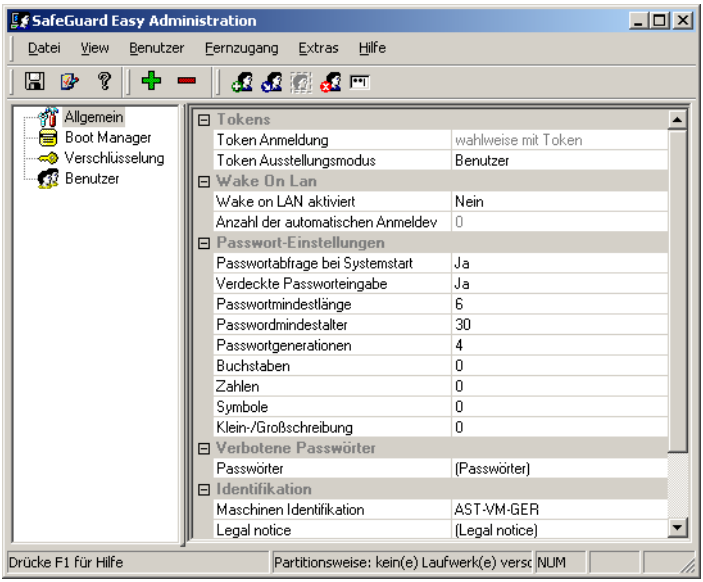
8.3 Die Administration

Nach dem Start der Administration erscheint eine Anmeldemaske, über die Daten in SafeGuard Easy eingegeben werden können, und verlangt vor dem Zugriff gültige SafeGuard Easy-Zugangsdaten.

Die Zahl der Anmeldeversuche ist auf fünf begrenzt. Danach muss das System neu gestartet werden, um sich erneut anzumelden.

8.3.1 Administrations-Fenster

Nach der korrekten Eingabe der SafeGuard Easy-Benutzerdaten öffnet sich das Administrations-Fenster.



Das linke Fenster zeigt eine Liste aller verfügbaren Konfigurationsseiten an. Wird im linken Fenster eine Konfigurationsseite ausgewählt, werden im rechten Fenster Details über Einstellungsmöglichkeiten angezeigt. Die verschiedenen Einstellmöglichkeiten entsprechen denjenigen, die während der Installation von SafeGuard Easy vorgenommen werden können.

Die Statusleiste des Administrationsfensters gibt weitere Informationen über:

- Verschlüsselungsmodus und der Verschlüsselungsstatus der Laufwerke (im Bild: Partitionsweise, keine Laufwerke verschlüsselt).
- Status der Tasten für den Nummernblock und die Hochstell-Taste (im Bild ist „Num Lock“ aktiviert)

In der Grundeinstellung darf jeder an der Administration angemeldete Benutzer dort sein SafeGuard Easy Passwort ändern. Der weitere Handlungsspielraum hängt von seinem Rechteprofil ab.

8.3.2 Symbol- und Werkzeugleiste

Die Administration verfügt über eine Symbolleiste mit Schaltflächen für die wichtigsten Kommandos (v.l.n.r.):

- **Speichern**
  Speichert neue Einstellungen. Verlangen geänderte Einstellungen nach einem Neustart, wird ein Dialog angezeigt.

- **Arbeitsbereich**
  Erlaubt, die Administration bei der nächsten Anmeldung wieder so vorzufinden, wie sie verlassen wurde (gleiche Größe/Position des Fensters, gleiche Konfigurationsseite etc.).

- **Hilfe**
  Zeigt die Onlinehilfe an.

- **Plus-/Minus-Zeichen**
  Das Plus-Zeichen zeigt im rechten Fenster alle untergeordneten Einstellungen, das Minuszeichen minimiert die Ansicht auf die Einstellungsüberschriften.

- **Benutzer anlegen**
  Fügt einen neuen Benutzer hinzu (Anzeige abhängig vom Rechteprofil des angemeldeten Benutzers).

- **Benutzer kopieren**
  Dupliziert einen vorhandenen Benutzer (Anzeige abhängig vom Rechteprofil des angemeldeten Benutzers).

- **Benutzer löschen**
  Entfernt den Benutzer aus der Liste (Anzeige abhängig vom Rechteprofil des angemeldeten Benutzers).

- **Passwort ändern**
  Erlaubt dem angemeldeten Benutzer, sein Passwort zu ändern.

All diese Kommandos sind auch über die verschiedenen Menüs (Datei, Ansicht, Benutzer, Extras, Hilfe) aufrufbar.

8.4 Konfigurationsdateiassistent

Die einzige Aufgabe des Konfigurationsdateiassistenten ist es, Dateien zu erzeugen, mit deren Hilfe die Installation und Deinstallation von SafeGuard Easy automatisiert werden kann. Auch administrative Aufgaben wie das Ändern einer bestehenden SafeGuard Easy Installation lassen sich über Konfigurationsdateien lösen. In Netzwerkumgebungen schickt der Administrator die Konfigurationsdateien an die Benutzer-PCs und lässt sie dort ohne Benutzerinteraktion ausführen. Nach Ausführen derselben Konfigurationsdatei an mehreren PCs arbeitet SafeGuard Easy an diesen Rechnern mit der gleichen Konfiguration.

Eine Konfigurationsdatei ist systemunabhängig, kann also auch auf anderen Systemen als jenem, auf dem sie generiert wurde, eingesetzt werden. Nur die auf den verschiedenen Systemen verwendete SafeGuard Easy-Version muss identisch sein.

HINWEISE:

Um eine Konfigurationsdatei zu erzeugen, müssen Sie nur die Administrationswerkzeuge installieren.

Beim Erzeugen einer Konfigurationsdatei wird SafeGuard Easy nicht auf Ihrem Rechner installiert.

Konfigurationsdateien sollten, wie alle Elemente einer Systemadministration, vor unbefugtem Zugriff geschützt und z.B. Benutzern nicht zugänglich gemacht werden.

8.4.1 Konfigurationsdateien aus älteren SafeGuard Easy-Versionen wiederverwenden

Konfigurationsdateien aus älteren Versionen lassen sich problemlos einlesen und weiterbearbeiten, vorausgesetzt die Dateien

- wurden mit einem Konfigurationsdateiassistenten ab SafeGuard Easy 3.20 erstellt.
- besitzen den Dateityp „Installieren“.

Beim Laden einer älteren Datei zeigt SafeGuard Easy selbstverständlich auch die neuen Konfigurationsmöglichkeiten automatisch auf (neu seit Version 3.20 ist bspw. die Token-Anmeldung) und setzt sie auf die Standardwerte.

8.4.2 Neue Konfigurationsdatei erstellen

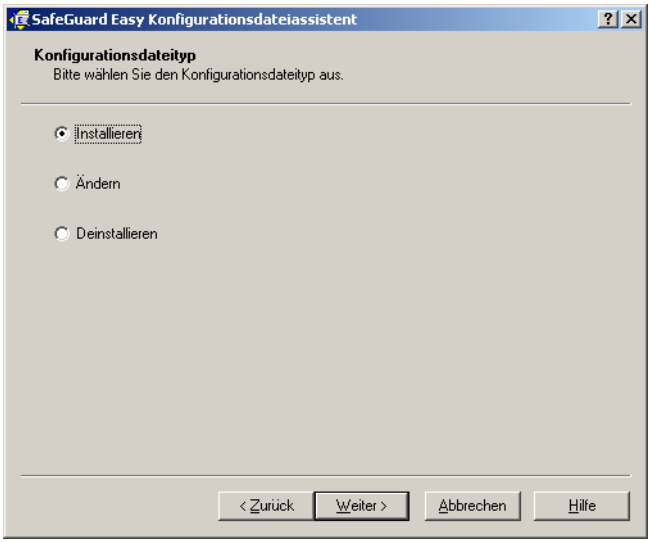
Mit Hilfe des Konfigurationsassistenten werden Dateien erzeugt, die Installation, Deinstallation und Änderungen ohne Benutzerinteraktion ablaufen lassen. Der Konfigurationsassistent erfasst schrittweise die Informationen, die eine Datei enthalten soll.

Neue Konfigurationsdateien werden erzeugt über Start / Programme / Utimaco / SafeGuard Easy / Konfigurationsdateiassistent.

Bestätigen Sie im Assistenten alle richtigen Eingaben mit [Weiter].

Nach dem Start wird zuerst festgelegt, zu welchem Zweck die Konfigurationsdatei erzeugt wird.

- Für eine Installation
- Für eine Änderung einer bestehenden SafeGuard Easy-Installation (sog. „Delta“-Datei)
- Für eine Deinstallation

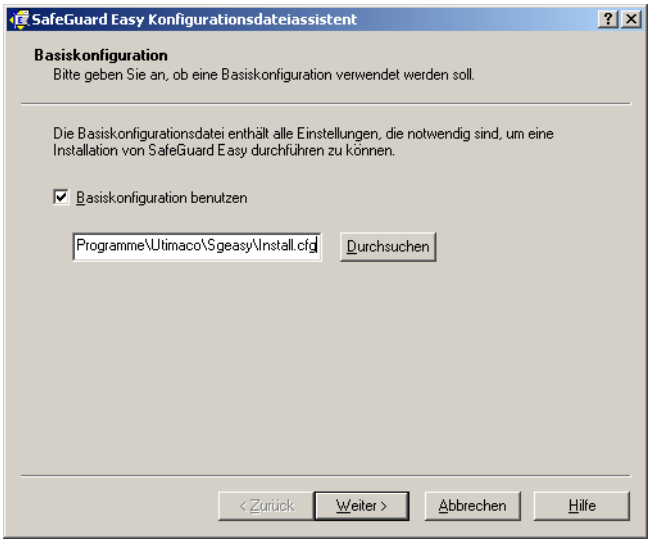


8.4.3 Konfigurationsdatei für Installation erstellen

Die Eigenschaft „Installieren“ erzeugt eine Konfigurationsdatei, mit der SafeGuard Easy automatisch auf einem Client installiert werden kann.

Nach Auswählen von „Installieren“ wählen Sie zuerst, ob für die neue Konfigurationsdatei eine Basiskonfiguration verwendet werden soll.

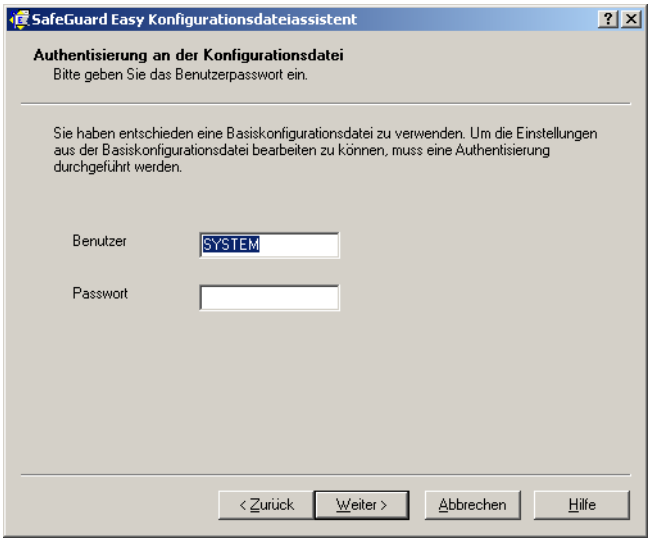
Basiskonfiguration


SafeGuard Easy Konfigurationsdateiassistent
Basiskonfiguration
Bitte geben Sie an, ob eine Basiskonfiguration verwendet werden soll.
Die Basiskonfigurationsdatei enthält alle Einstellungen, die notwendig sind, um eine Installation von SafeGuard Easy durchführen zu können.
Basiskonfiguration benutzen
Programme\Utimaco\Sgeasy\Install.cfg
Durchsuchen
< Zurück
Weiter >
Abbrechen
Hilfe

Eine Basiskonfigurationsdatei ist eine bereits bestehende Konfigurationsdatei mit der Eigenschaft „Installieren“. Sie kann als Grundlage für eine neue Installationsdatei geladen werden.

Authentisierung an der Basiskonfigurationsdatei (optional)

Die Einstellungen einer gewählten Basiskonfigurationsdatei werden erst nach der Anmeldung des SafeGuard Easy Benutzers SYSTEM sichtbar.

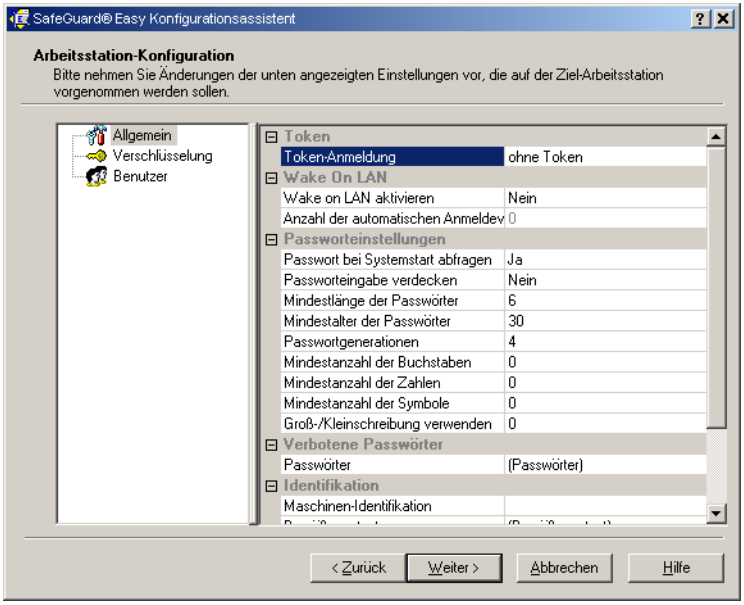

SafeGuard Easy Konfigurationsdateiassistent
Authentisierung an der Konfigurationsdatei
Bitte geben Sie das Benutzerpasswort ein.
Sie haben entschieden eine Basiskonfigurationsdatei zu verwenden. Um die Einstellungen aus der Basiskonfigurationsdatei bearbeiten zu können, muss eine Authentisierung durchgeführt werden.
Benutzer
SYSTEM
Passwort
< Zurück
Weiter >
Abbrechen
Hilfe

Verschlüsselungsmodus

Ohne Basiskonfiguration muss der neuen Konfigurationsdatei der Verschlüsselungsmodus mitgegeben werden, damit SafeGuard Easy weiß, welche Festplattenbereiche zu verschlüsseln sind (siehe Verschlüsselungsmodus').

Konfiguration

Anschließend folgt die Ansicht mit den verschiedenen Konfigurationsseiten. Mit einer Basiskonfigurationsdatei werden deren Einstellungen geladen, ohne Basiskonfiguration erscheinen die Standardeinstellungen.



Detaillierte Informationen zu den Konfigurationsseiten finden Sie in den entsprechenden Kapiteln.

Zielverzeichnis

Im Dialog *Zielverzeichnis* legen Sie fest, in welchem Pfad Sie eine neu erstellte Konfigurationsdatei speichern wollen.

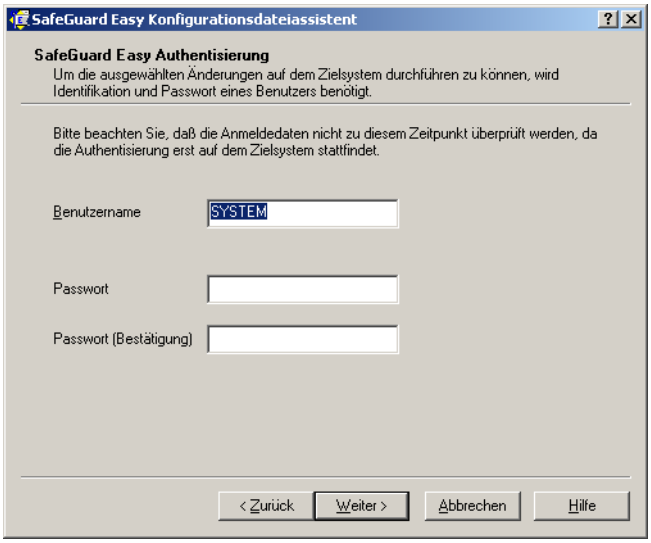
Um Probleme zu vermeiden, notieren Sie sich bitte immer die Eigenschaften und Einstellungen, die Sie einer Konfigurationsdatei zuweisen.

HINWEIS:
Bei einer Konfigurationsdatei vom Typ „Ändern mit Basiskonfiguration“ werden Sie nach dem Klick auf [Speichern] gefragt, ob Sie die angegebene, bereits existierende Basiskonfigurationsdatei ersetzen wollen. Wenn Sie [Ja] drücken, wird die Datei überschrieben und die Änderungen werden der bereits bestehenden Basiskonfigurationsdatei hinzugefügt.

Sie sollten die originale Basiskonfigurationsdatei behalten und eine neue Datei erzeugen. Benennen Sie einfach die Basiskonfigurationsdatei um und speichern Sie sie unter anderem Namen ab.

8.4.4 Konfigurationsdatei zur Deinstallation erstellen

Der Konfigurationstyp „Deinstallieren“ öffnet den Dialog SafeGuard Easy Authentisierung.


SafeGuard Easy Konfigurationsdateiassistent
SafeGuard Easy Authentisierung
Um die ausgewählten Änderungen auf dem Zielsystem durchführen zu können, wird Identifikation und Passwort eines Benutzers benötigt.
Bitte beachten Sie, daß die Anmeldedaten nicht zu diesem Zeitpunkt überprüft werden, da die Authentisierung erst auf dem Zielsystem stattfindet.
Benutzername
SYSTEM
Passwort
Passwort (Bestätigung)
< Zurück
Weiter >
Abbrechen
Hilfe

Der hier eingetragene Benutzer muss über das Recht zur Deinstallation verfügen.

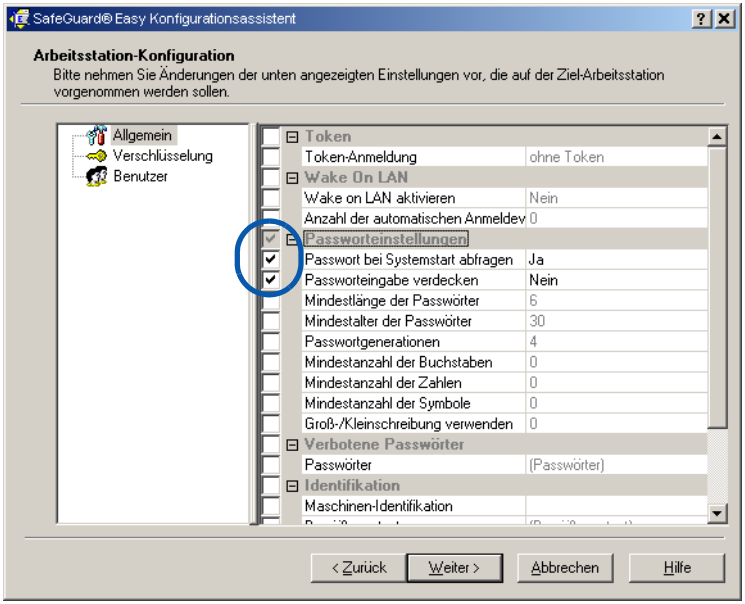
Nach der Dateneingabe springt der Assistent über [Weiter] zum Dialog *Zielverzeichnis*. Dort geben Sie der Konfigurationsdatei einen Namen.

8.4.5 Konfigurationsdatei für Änderung („Delta-Datei“) erstellen

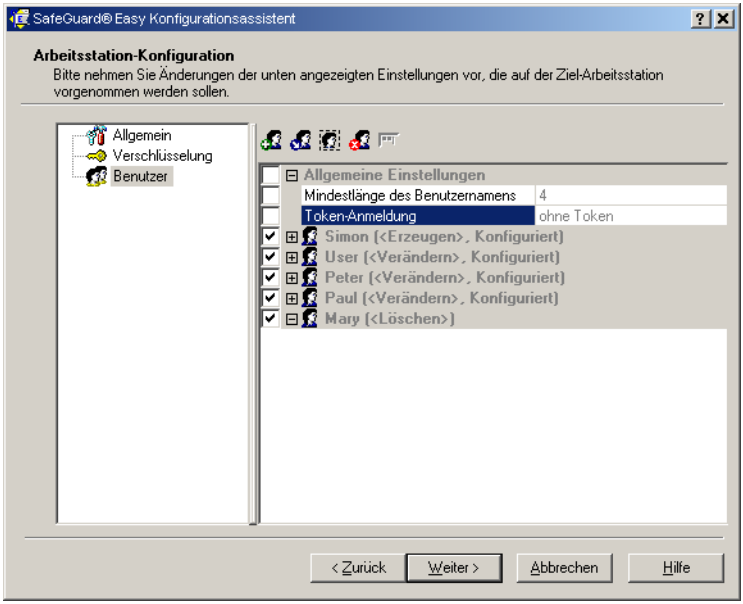
Kurz gesagt ändert eine Delta-Datei die Einstellungen einer bestehenden SafeGuard Easy-Installation. Wie eine Installationsdatei, kann auch eine Delta-Datei mit oder ohne Basiskonfiguration erstellt werden.

Im Gegensatz zur Installationsdatei ist es in Delta-Dateien aber nicht möglich, den Status der Festplattenverschlüsselung und der Token-Unterstützung zu ändern.

Die Optionen auf den einzelnen Konfigurationsseiten sind bei Delta-Dateien erst bearbeitbar, nachdem das entsprechende Auswahlkästchen angeklickt wurde.



Beachten Sie auf der Konfigurationsseite *Benutzer* bitte die Funktionalitäten der Schaltflächen zum Anlegen, Kopieren und Löschen von Benutzern.



- **Benutzer erzeugen**
  Erzeugt beim Ausführen der Konfigurationsdatei einen neuen SafeGuard Easy-Benutzer mit diesem Namen (im Beispiel Benutzer *Simon*).

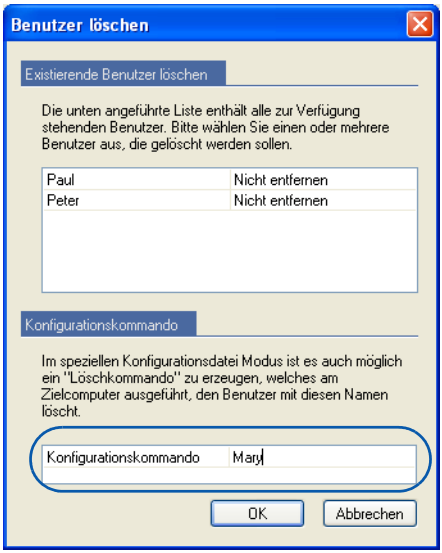
- **Benutzer kopieren**
  Übernimmt sämtliche Einstellungen des kopierten Eintrags, und der neue SafeGuard Easy-Benutzer erhält ebenfalls das Attribut „Erzeugen“.

- **Benutzer verändern**
  Erzeugt einen Benutzer, der bereits auf einer Arbeitsstation vorhanden ist und weist ihm neue Eigenschaften zu (im Beispiel Benutzer *User, Peter* und *Paul* mit dem Attribut „Verändern“).

Alle aus einer Basiskonfiguration geladenen Benutzer besitzen automatisch die Eigenschaft „Verändern“. Ohne Basiskonfiguration müssen Benutzer mit dieser Eigenschaft erst erzeugt werden.

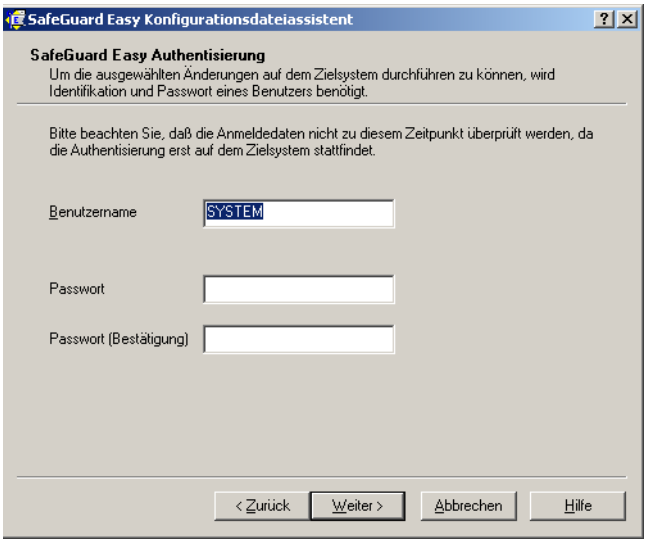
- **Benutzer löschen**
  Gibt den Namen eines bestehenden Benutzers an, der beim Ausführen der Konfigurationsdatei auf diesem Zielsystem entfernt wird (im Beispiel Benutzerin *Mary*).

HINWEIS:
In Delta-Dateien ohne Basiskonfiguration ist Benutzern über das Feld „Konfigurationskommando“ die Eigenschaft „Löschen“ zuzuweisen.


Benutzer löschen
Existierende Benutzer löschen
Die unten angeführte Liste enthält alle zur Verfügung stehenden Benutzer. Bitte wählen Sie einen oder mehrere Benutzer aus, die gelöscht werden sollen.
Paul
Nicht entfernen
Peter
Nicht entfernen
Konfigurationskommando
Im speziellen Konfigurationsdatei Modus ist es auch möglich ein "Löschkommando" zu erzeugen, welches am Zielcomputer ausgeführt, den Benutzer mit diesen Namen löscht.
Konfigurationskommando
Mary
OK
Abbrechen

Nach der Dateneingabe gelangt man über [Weiter] zum Dialog Authentisierung und dann zum *Zielverzeichnis*.

Authentisierung


SafeGuard Easy Konfigurationsdateiassistent
SafeGuard Easy Authentisierung
Um die ausgewählten Änderungen auf dem Zielsystem durchführen zu können, wird Identifikation und Passwort eines Benutzers benötigt.
Bitte beachten Sie, daß die Anmeldedaten nicht zu diesem Zeitpunkt überprüft werden, da die Authentisierung erst auf dem Zielsystem stattfindet.
Benutzername
SYSTEM
Passwort
Passwort (Bestätigung)
< Zurück
Weiter >
Abbrechen
Hilfe

Der hier eingetragene SafeGuard Easy-Benutzer muss auf der Arbeitsstation, auf der die Konfigurationsdatei ausgeführt wird, vorhanden sein und über entsprechende Rechte verfügen.

8.4.6 Delta-Datei ausführen

Im Gegensatz zu Konfigurationsdateien zur Installation, Deinstallation und Migration erfordert das Ausführen einer Delta-Datei einen speziellen Kommandozeilenaufruf.

1. Wechseln Sie zur Eingabeaufforderung, oder rufen Sie den Befehl **Ausführen** im Windows-Startmenü auf.
2. Wechseln Sie in das SafeGuard Easy-Verzeichnis.
3. Geben Sie den Befehl

   `EXECCFG.exe /f:`*<Pfad / Name der Konfigurationsdatei>*

   ein und klicken Sie anschließend auf [OK].

   `EXECCFG` unterstützt folgende Parameter:

`/REBOOT`	Neustart nach Ausführen der Konfigurationsdatei
`/?`	Zeigt alle Parameter an

BEISPIEL:

```
C:\SGEasy\EXECCFG /f:D:\Delta.cfg /Reboot
```

Mit diesem Befehl wird die Konfigurationsdatei Delta.cfg aufgerufen. Danach erfolgt ein Neustart.

ACHTUNG:
Zwischen „/f“ und dem Verzeichnisnamen der Delta-Datei darf KEIN LEERZEICHEN stehen.

8.4.7 Konfigurationsdatei editieren

Die Einstellungen von Konfigurationsdateien mit der Eigenschaft „Installieren“ können auch nach dem Abspeichern nachträglich geändert werden.

Um eine Konfigurationsdatei zu verändern, gehen Sie wie folgt vor:

1. Starten Sie den Konfigurationsdateiassistenten.
2. Wählen Sie als Dateityp „Installieren“ und laden Sie die zu editierende Datei im Dialog *Basiskonfiguration*.
3. Mit einem Klick auf [Weiter] wird die Konfigurationsdatei gelesen.
4. Die darin abgespeicherten Einstellungen werden angezeigt und können verändert werden.

Wird versucht, eine Datei mit der Eigenschaft „Ändern“ oder „Entfernen“ aufzurufen, wird eine Fehlermeldung ausgegeben.

8.4.8 Anwendungsbeispiele

Beispiel 1:

Erzeugen Sie im Konfigurationsdateiassistenten eine Datei, mit der SafeGuard Easy ohne Benutzerinteraktion auf mehreren Arbeitsstationen eines Unternehmens installiert werden kann. Die Konfigurationsdatei soll zusätzlich ein hierarchisches Administrationskonzept unterstützen und folgende Benutzerprofile beinhalten:

- SYSTEM: SafeGuard Easy-Administrator, der alle Rechte besitzt
- SUBADMIN: Unterverwalter, an den administrative Aufgaben delegiert werden; er darf Benutzereinstellungen ändern und die Diskettenverschlüsselung schalten.
- USER: Endbenutzer, der über keine Rechte verfügt

Vorgehensweise:

1. Konfigurationsdateiassistent starten.
2. Konfigurationsdateityp „Installieren“ wählen.
3. Keine Basiskonfiguration wählen.
4. Verschlüsselungsmodus „Festplatten Verschlüsselung“ wählen.
5. Unter „Allgemein“ die Option „Passwort beim Systemstart abfragen“ wählen.
6. Unter "Benutzer" folgende Einstellungen treffen:
   - SYSTEM (Passwort: System)
     Rechte: Alle
   - SUBADMIN (Subadmin)
     Verkürzten C/R Code erzeugen: JA
     Rechte:
     - Benutzereinstellungen ändern
     - Diskettenverschlüsselung schalten
   - USER (User)
     Rechte: Keine
7. Unter Verschlüsselungseinstellungen folgende Einstellungen treffen:

   Diskettenverschlüsselung: Aktivieren
   Festplattenverschlüsselung: Aktivieren
   Wechselmedienverschlüsselung: Aktivieren
8. Unter MBR-Einstellungen Standardeinstellungen übernehmen.
9. Unter Zielverzeichnis Basiskonfigurationsdatei „Install.cfg“ speichern.
10. Install.cfg verteilen.

Beispiel 2:

Basierend auf der Install.cfg aus Beispiel 1 soll nun auf allen Arbeitsstationen der Benutzer „User“ temporär den Diskettenschlüssel ändern dürfen. Gemäß der festgelegten Administrationsstrukturen wird dieses Recht von dem Benutzer „SUBADMIN“ gewährt. Um dies zu erreichen, muss der SUBADMIN eine Konfigurationsdatei vom Typ „Ändern“ erzeugen und diese an die entsprechenden Arbeitsstationen verteilen.

Vorgehensweise:

1. Konfigurationsdateiassistent starten
2. Konfigurationsdateityp „Ändern“ wählen.
3. Als Basiskonfiguration „Install.cfg“ wählen.
4. Bei der Authentisierung an Konfigurationsdatei mit SUBADMIN (Passwort: subadmin) anmelden.
5. Bei Benutzereinstellungen
   - Unter „USER“ den Punkt „Rechte“ doppelklicken.
   - Diskettenverschlüsselung schalten aktivieren
6. Unter Zielverzeichnis „Change.cfg“ speichern.
7. Change.cfg auf Benutzer-PC verteilen.

8.5 Konfigurationsdatei über Kommandozeile erzeugen

Wenn Sie eine Konfigurationsdatei über die Kommandozeile erzeugen wollen, nutzen Sie das Programm `CfgWiz.exe`. `CfgWiz` ist im SafeGuard Easy-Verzeichnis zu finden.

`CfgWiz` kann mit folgenden Parametern aufgerufen werden:

`/cmd:install | change | uninstall`

Diese Option ersetzt den Dialog Konfigurationsdateityp.

`/base:<filename>`

Diese Option benennt die Basiskonfiguration, die genutzt werden soll. Bei einer Install-Datei ersetzt diese Option den Basiskonfigurationsdatei-Dialog.

`/instfile:<filename>`

Diese Option benennt den Namen der der Install-Datei, die erzeugt werden soll. Wenn dieser Parameter vorhanden ist, erscheint der Dialog Zielverzeichnis nicht. Wenn die Datei bereits existiert, wird sie mit der neuen Konfiguration überschrieben.

`/changefile:<filename>`

Diese Option benennt den Namen der der Delta-Datei, die erzeugt werden soll. Wenn dieser Parameter vorhanden ist, erscheint der Dialog Zielverzeichnis nicht. Wenn die Datei bereits existiert, wird sie mit der neuen Konfiguration überschrieben.

`/uninstfile:<filename>`

Diese Option benennt den Namen der Deinstallationsdatei, die erzeugt werden soll. Wenn dieser Parameter vorhanden ist, erscheint der Dialog Zielverzeichnis nicht. Wenn die Datei bereits existiert, wird sie mit der neuen Konfiguration überschrieben.

Beispiel:

```
CfgWiz /cmd:change /base:C:\install.cfg /changefile:C:\Change.cfg
```

HINWEIS:
In zukünftigen Versionen von LANDesk Management Systems werden diese Funktionen möglicherweise enthalten sein.

8.6 Häufig verwendete Registry-Einstellungen für SafeGuard Easy über die administrative Vorlage ändern

Um den Komfort bei der Konfiguration zu steigern, hat Utimaco eine eigene administrative Vorlage für den Gruppenrichtlinieneditor (Gpedit.msc) erstellt. Mit dieser Vorlage (Dateiname: Sguard_0407.adm) lassen sich bestimmte SafeGuard Easy-Einstellungen bequem vornehmen, ohne die Registry bearbeiten zu müssen.

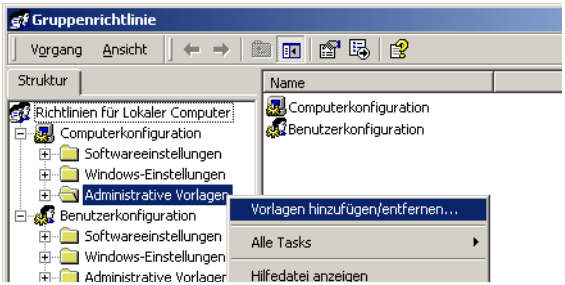
> ***HINWEIS:***
> Die administrative Vorlage wird nur bei einer SafeGuard Easy Client-Installation angelegt!

Die Einstellungen der administrativen Vorlage für einen Benutzer-PC ändert ein Administrator lokal über den Gruppenrichtlinieneditor (Gpedit.msc) oder zentral über Gruppenrichtlinienobjekte (GPOs) in einer Active Directory-Umgebung. Benutzer haben in einer IT-Umgebung gewöhnlich keine Administratorrechte, können demzufolge selbst die SafeGuard Easy-Richtlinien nicht ändern.

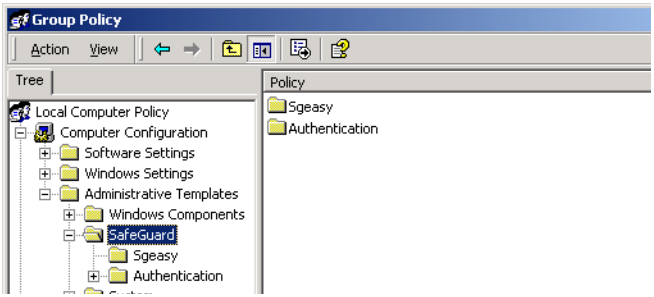
Im folgenden eine Kurzanleitung, wie die Utimaco-Vorlage in ein lokales System eingebunden wird. Die Handhabung administrativer Vorlagen in einer Active Directory-Umgebung mit GPOs lesen Sie bitte in der gängigen Microsoft Dokumentation nach.

1. Als Benutzer mit Windows-Administratorrechten anmelden.
2. Unter Start / Ausführen das Kommando „gpedit.msc“ eingeben und den lokalen Gruppenrichtlinieneditor starten.
3. Die SafeGuard-Vorlage **Sguard_0407.adm** über „Administrative Vorlagen“ > „Vorlagen hinzufügen“.

Sguard_0407.adm ist abgelegt im SafeGuard Easy-Installationsverzeichnis im Ordner \ADM.



4. Neben den bisherigen Ordnern erscheint der Ordner „SafeGuard“ in der Computerkonfiguration.



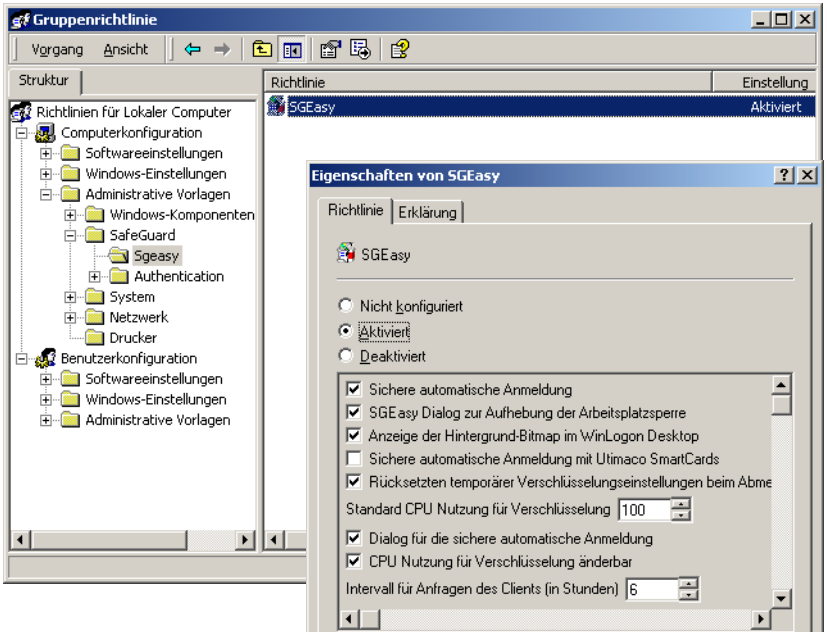
5. Bei Nicht-Windows-Vorlagen stellt die vorkonfigurierte Ansicht ein Problem da. Deswegen muss zur Ansicht der einzelnen Richtlinien folgende Einstellung vorgenommen werden:

   Windows 2000:
   Ordner „Administrative Vorlagen“ markieren > Menü „Ansicht“ > Haken vor „Nur Richtlinien anzeigen“ entfernen.

   Windows XP/Windows Server 2003:
   Ordner „Administrative Vorlagen“ markieren > Menü „Ansicht“ > „Filtern“ > Haken vor „Nur konfigurierte Richtlinien anzeigen“ entfernen.

6. Richtlinie per Doppelklick öffnen und unter „Eigenschaften von SGEasy“ Einstellungen vornehmen.

.



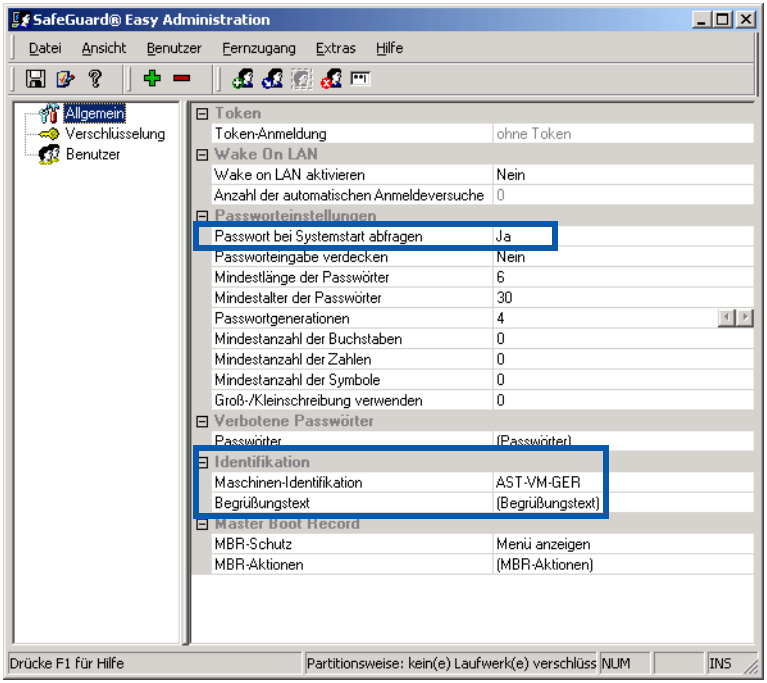
Die Richtlinien können drei verschiedene Status annehmen:

- **Nicht konfiguriert**
  Die aktuellen Einstellungen beim Benutzer werden nicht verändert, d.h. früher gemachte Einstellung bleiben.

- **Aktiviert**
  Die Einstellungen werden übernommen.

- **Deaktiviert**
  Die Einstellungen werden aktiv entfernt.

9 Pre-Boot Authentisierung



Bei der Pre-Boot Authentisierung handelt es sich um eine Anmeldefunktionalität, die eine Authentisierung vor dem Bootprozess verlangt. Weitere Informationen über die Pre-Boot Authentisierung lesen Sie bitte unter Systemstart und Anmeldung' nach.

Definiert werden die Pre-Boot Authentisierung-Einstellungen über die Konfigurationsseite ALLGEMEIN.

9.1 Sprache der Pre-Boot Authentisierung nachträglich ändern

Der Anmeldebildschirm übernimmt die bei der Installation gewählte Sprache (Deutsch, Englisch oder Französisch). Benutzer müssen SafeGuard Easy nun nicht mehr deinstallieren, um die Texte der Pre-Boot Authentisierung in einer anderen Sprache darzustellen.

> ***ACHTUNG:***
> Es lassen sich nachträglich nur die in der Pre-Boot Authentisierung angezeigten Texte ändern, nicht das Tastaturlayout!

Parameter für die Sprachänderung

SetPBALang kann mit folgenden Parametern aufgerufen werden:

```
SetPBALang [en | de | fr] | [n]
```

`[en | de | fr]`	Setzt die neue Sprache fest
`[n]`	Verwendet eine Nummer (1-255) für die Spracheinstellung Folgende Sprachen werden unterstützt: 9=Englisch 7=Deutsch 12=Französisch

Nach einem Neustart ist die Spracheinstellung geändert.

SetPBALang finden Sie im Programmverzeichnis von SafeGuard Easy.

9.2 Passwort beim Systemstart abfragen

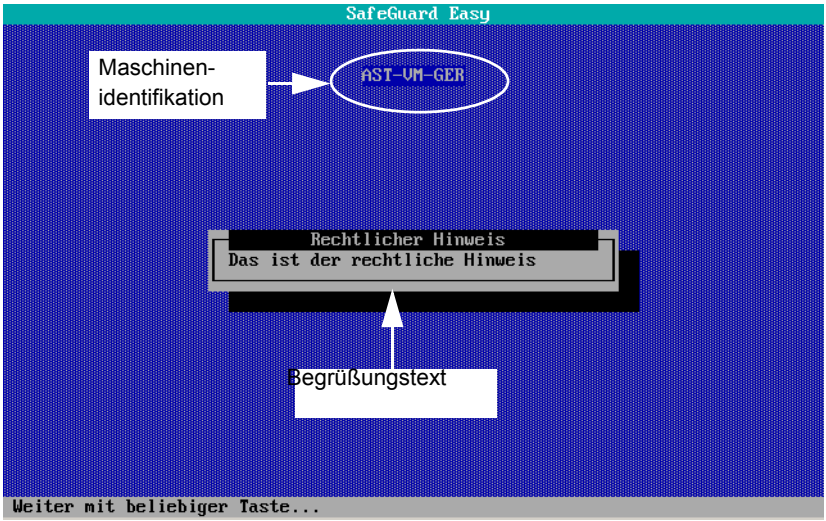
Die Option „Passwort beim Systemstart abfragen“ schaltet die Pre-Boot Authentisierung ein/aus. Ist die Pre-Boot Authentisierung eingeschaltet, wird ein Anmeldebildschirm angezeigt, bevor das Betriebssystem geladen wird. Erst nach erfolgreicher Authentisierung mit den korrekten SafeGuard Easy-Zugangsdaten startet Windows.

Schalten Sie die Pre-Boot Authentisierung aus, ist keine Anmeldung vor dem Systemstart erforderlich. Die Authentisierung erfolgt dann wie gewohnt über den Anmeldedialog des Betriebssystems.

Aus Sicherheitsgründen sollten Sie die Pre-Boot Authentisierung nie deaktivieren!

9.3 Identifikation

Die Optionen unter „Identifikation“ erlauben, in der Pre-Boot Authentisierung frei definierbare Texte einzublenden.



9.3.1 Maschinen Identifikation

Der in diesem Feld eingetragene Name/Text erscheint im Pre-Boot Authentisierung-Anmeldedialog. Wurde bereits ein Maschinenname in den Windows-Netzwerkeinstellungen eingetragen, wird dieser in der Grundeinstellung automatisch übernommen.

Es können maximal 63 Zeichen eingegeben werden.

Die Maschinen Identifikation kann auch Verknüpfungen zu Umgebungsvariablen enthalten. Diese Verknüpfungen werden bei der Installation aufgelöst. Nützlich ist dies vor allem bei der Erstellung von Konfigurationsdateien, die auf mehreren Arbeitsstationen installiert werden.

BEISPIEL:

Der Eintrag in das Feld „Maschinenidentifikation“

Das ist %USERDOMAIN%. Es wird von %WINDIR% gebootet.

wird von Windows aufgelöst zu

Das ist PC1234. Es wird von C:\WINNT gebootet.

Es gibt für alle Betriebssysteme die spezielle Variable %COMPUTERNAME%. Mit dieser wird plattformunabhängig der Computername eingebunden. Die Variable %COMPUTERNAME% wird immer zum NETBIOS Namen des Computers aufgelöst.

Zusätzlich gelten folgende Regeln:

- Undefinierte Umgebungsvariablen ergeben leere Verknüpfungen.
- Wenn die Variable für das Maschinen Identifikationsfeld zu lang ist, wird sie zu „[...]“ aufgelöst.
- Bei Variablennamen muss die Groß-/Kleinschreibung nicht beachtet werden.
- Wenn ein Prozentzeichen in der Verknüpfung notwendig ist, verwenden Sie „%%“.
- Die Auflösung von Variablen wird nur einmal während der Installation durchgeführt, nicht bei jedem Neustart des Computers.

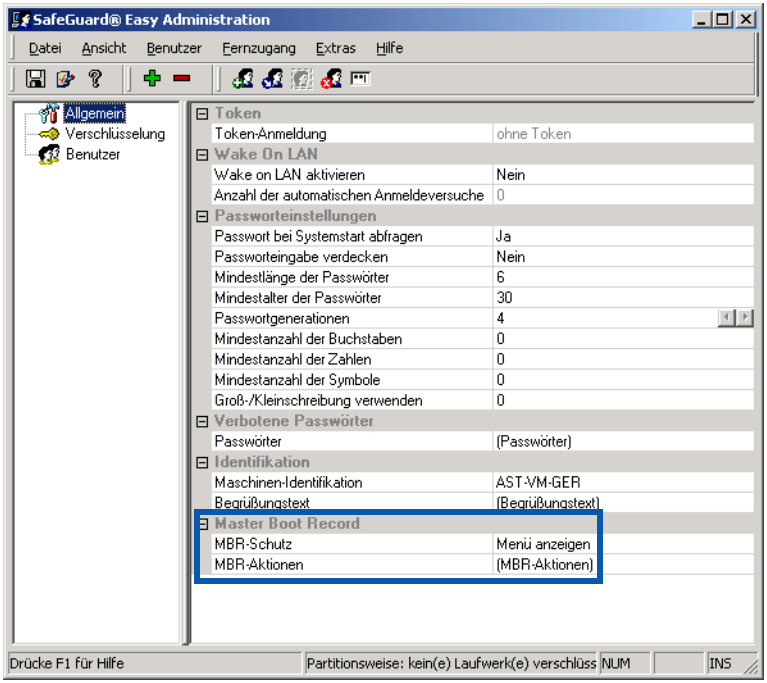
9.3.2 Begrüßungstext

Hier handelt es sich um eine Textbox mit frei konfigurierbarem Inhalt, die in der Pre-Boot Authentisierung vor der Anmeldung mit den SafeGuard Easy-Zugangsdaten erscheint. In manchen Ländern ist das Erscheinen eines Textfeldes mit bestimmtem Inhalt gesetzlich vorgeschrieben.

Der Titel kann bis zu 68 Zeichen umfassen, der Textblock bis zu 10 Zeilen mit jeweils 70 Zeichen.

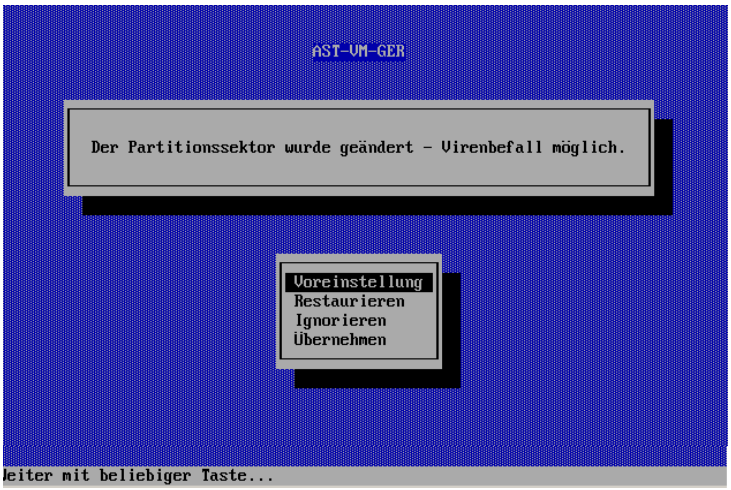
Die Box muss vom Benutzer bestätigt werden, bevor das System fortfährt.

10 Master Boot Record



Im Master Boot Record (MBR) einer Festplatte werden für jede angelegte Partition verschiedene Informationen gespeichert. Durch ihn erfährt das System, welche Festplatte beziehungsweise welche Partition zum Booten verwendet wird. Er ist daher ein beliebter Angriffspunkt für Viren, da das BIOS den darin enthaltenen Maschinencode ganz zu Beginn des Bootvorgangs ausführt, noch bevor das Betriebssystem geladen wird.

SafeGuard Easy kann Modifikationen am MBR erkennen und darauf in verschiedener Art und Weise reagieren, z.B. ein Menü anzeigen und den Benutzer die Reaktion auswählen lassen.



Definiert werden die Einstellungen des Master Boot Record auf der Konfigurationsseite „ALLGEMEIN“.

10.1 MBR-Schutz

Der MBR-Schutz bietet einen Schutzmechanismus gegen Viren, die den Partitionssektor befallen. Sofern Sie nicht „Änderungen ignorieren“ eingestellt haben, wird der MBR bei jedem Systemstart auf Veränderungen überprüft.

- **Änderungen ignorieren**
  Bei dieser Einstellung wird eine mögliche Veränderung des MBR akzeptiert. Der Bootprozess wird nicht unterbrochen.

- **Menü anzeigen**
  Bei einer Veränderung des MBR wird ein Menü anzeigt, über das Sie eine der folgenden Aktionen wählen können:

  - Voreinstellung
  - Restaurieren
  - Ignorieren
  - Übernehmen

  Mit *Voreinstellung* wählt der Benutzer die definierte Standardaktion (siehe ’MBR (Standard) Aktionen’), mit *Restaurieren* wird der MBR aus der Sicherheitskopie restauriert, mit *Ignorieren* wird die Veränderung übergangen und mit *Übernehmen* wird der aktuelle MBR akzeptiert.

  Die Überprüfung des MBR auf Veränderungen findet vor der Benutzeranmeldung statt. Das Menü wird aber erst nach einer gültigen Anmeldung angezeigt. Damit ist ausgeschlossen, dass ein nicht autorisierter Benutzer entscheiden kann, was in diesem Fall geschehen soll.

- **Standardaktionen durchführen**
  Hierbei werden die unter **MBR Aktionen** definierten Standardaktionen durchgeführt.

10.2 MBR (Standard) Aktionen

Sie können eine oder mehrere Standardaktionen auswählen:

- **Warnung anzeigen**
  Dem Benutzer wird mitgeteilt, dass der für SafeGuard Easy erstellte MBR modifiziert wurde. Der Benutzer muss diese Meldung durch Tastendruck bestätigen.

- **MBR restaurieren**
  Der Original-MBR wird ohne Benachrichtigung des Benutzers aus der Sicherheitskopie wiederhergestellt um einen möglichen Virus zu entfernen. Danach startet das System neu.

- **System anhalten**
  Bei einer Veränderung des MBR wird im Benutzer-Status nach der Anmeldung eine Nachricht angezeigt und das System angehalten. Es ist nun nicht mehr möglich, die Arbeitsstation zu booten, und der Benutzer ist gezwungen, die Hilfe des Administrators bzw. des Supports anzufordern.

  Hat sich der Benutzer SYSTEM angemeldet, wird die Kopie automatisch durch den Original-MBR ersetzt und der Rechner bootet ohne das System zu stoppen.

10.3 Unterstützung für Compaq Setup-Partition

Diese Option lässt den MBR weitgehend unverändert. Dies ist auf verschiedenen Compaq-Systemen (und eventuell anderen) erforderlich, um den Zugriff auf die Setup-Partition zu ermöglichen. Sie können, obwohl SafeGuard Easy installiert ist, bei COMPAQ-Notebooks die Wartungsposition booten. Wollen Sie den Original MBR beibehalten, klicken Sie auf „Ein“, nachdem Sie den Menüpunkt markiert haben. Deaktiviert wird die Einstellung durch einen Klick auf „Aus“. Diese Option kann bei allen Verschlüsselungsmodi (Standard, Bootschutz, Partitionsweise) ein- bzw. ausgeschaltet werden.

Da diese Option nur in Zusammenhang mit Compaq Setup-Partitionen von Bedeutung ist, wird sie in der Administration nur angezeigt, wenn sich auf der Festplatte eine solche Partition befindet und die Partitionstabelle im MBR der ersten Festplatte noch mindestens einen freien Eintrag aufweist. Im Konfigurationsdatei-Assistenten steht diese Option immer zur Auswahl zur Verfügung.

HINWEIS:
Utimaco rät, diese Option nur dann zu wählen, wenn sie unbedingt benötigt wird. Dies betrifft verschiedene Compaq-Modelle. Sind Sie nicht sicher, wie Ihr Rechner reagiert, kontaktieren Sie bitte die Compaq Hotline.

11 Verschlüsselung

Das Kernstück von SafeGuard Easy ist die Verschlüsselung von Daten auf unterschiedlichen Datenträgern, nämlich Festplatten-, Disketten- und Wechselmedienlaufwerken.

Die Verschlüsselung von Disketten- und Wechselmedienlaufwerken bietet den Vorteil, dass die gesamte Datenkommunikation mit der Außenwelt verschlüsselt abläuft. Auf einem PC mit aktivierter Verschlüsselung sind reguläre Klartext-Disketten nicht lesbar. Nicht lesbare Disketten müssen erst im verschlüsselten Laufwerk neu formatiert werden, bevor sie benutzt werden können. Nach einer Formatierung gehen jedoch alle Daten verloren! Werden Disketten zwischen verschiedenen Arbeitsstationen ausgetauscht, müssen die Laufwerke der betreffenden Arbeitsplätze mit identischem Algorithmus und Schlüssel verschlüsselt sein. Ist dies nicht der Fall, kann das Medium nicht gelesen werden.

Benutzer mit entsprechenden Rechten können die Disketten- und Wechselmedienschlüssel temporär ändern, vorausgesetzt die Verschlüsselung ist aktiviert (siehe 'Disketten- und Geräteverschlüsselung schalten').

Die Verschlüsselung mit jeweils unterschiedlichen Schlüsseln kann in verschiedenen Algorithmen (AES-128, AES-256, Rijndael-256, IDEA, DES, 3DES, DES SB-II, Blowfish-8, Blowfish-16, STEALTH-40, XOR und XOR SB-I A=B) durchgeführt werden. Der Schlüssel wird nach seiner Definition verschlüsselt und aus Sicherheitsgründen nicht im System abgelegt. Er wird jeweils beim Booten aus einem auf der Festplatte gespeicherten Code und dem SafeGuard Easy Passwort des Benutzers neu generiert.

Neben der Verschlüsselung von maximal vier Festplatten können wahlweise auch nur die Systembereiche oder einzelne Partitionen verschlüsselt werden. Unterstützt werden folgende Dateisysteme: FAT-12, FAT-16, FAT-32, HPFS, NTFS und NTFS5. Die Anzahl der verschlüsselbaren Partitionen einer Festplatte ist auf acht begrenzt.

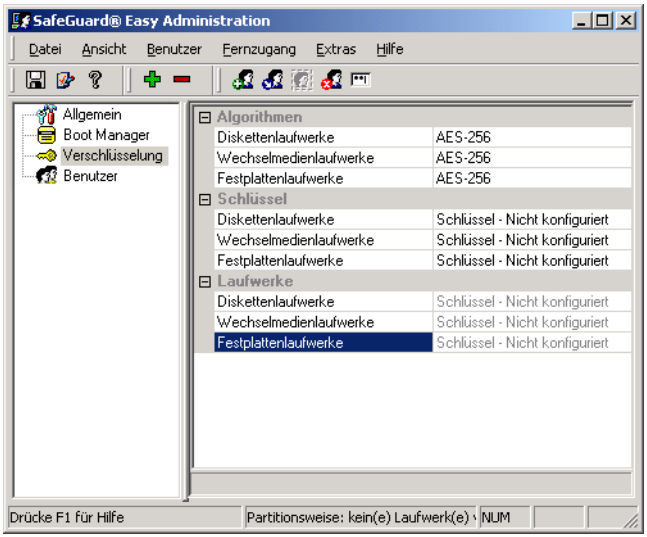
Zur Feinabstimmung des Zugriffsschutzes auf Ihrem System empfehlen wir Ihnen folgende Module aus der SafeGuard-Produktfamilie:

- **Anwendungsspezifische Zugriffsrechte (ASAR):**
  Realisiert ein 3-dimensionales Sicherheitskonzept, das es ermöglicht, explizite Rechte zwischen den Benutzern, Daten und Anwendungen zu spezifizieren. Dies stellt einen Schutz gegen die Bedrohung durch bestimmte (sogar momentan noch unbekannte) Viren dar und implementiert ein hohes Maß an Sicherheit auch in unverwaltetem Code oder Umgebungen mit gemischten Windows-Versionen.

- **Plug&Play Management (PnP):**
  Benutzer können beliebige PnP-Geräte, wie z.B. USB-Speichersticks, anstecken und sofort nutzen. Das PnP Management ermöglicht einen kontrollierten Datenimport/-export auf Speichermedien auf Klassenebene und für einzelne Geräte.

11.1 Verschlüsselung konfigurieren

Die Verschlüsselungseinstellungen werden in den Verwaltungsprogrammen auf der Konfigurationsseite „Verschlüsselung“ gesetzt.



11.2 Unterstützte Festplattenlaufwerke

- IDE/SCSI Festplatten
- Serial-ATA Festplatten (hot pluggable)
- Firewire Festplatten (hot pluggable)
- USB Festplatten (hot pluggable)

HINWEISE ZUR FESTPLATTENVERSCHLÜSSELUNG:

- **Hot-Pluggable Festplatten**

  Alle Festplatten, die verschlüsselt werden sollen, müssen bei der Installation von SafeGuard Easy bereits mit dem PC verbunden sein.

  Die Erstverschlüsselung von hot-pluggable Festplatten darf nicht unterbrochen werden.

  Auch beim ersten Neustart nach der Erstverschlüsselung müssen die hot-pluggable Festplatten noch angeschlossen sein. Nach der Erstverschlüsselung kann das Laufwerk nach Bedarf angeschlossen und wieder entfernt werden. Vorausgesetzt der Benutzer nimmt immer wieder ein und dieselbe Festplatte z.B. für regelmäßige Datenbackups, sind i.d.R. keine Probleme zu erwarten.

  Werden mehrere Festplatten genutzt (z.B. eine verschlüsselte Festplatte entfernt und danach eine unverschlüsselte angeschlossen), kann dies Probleme nach sich ziehen, z.B. die SafeGuard Easy Verschlüsselungstabelle durcheinander bringen.

Grundsätzlich gilt: Die Disknumerierung (Disk Management) bei Gebrauch muss der Numerierung während des Installationsvorganges bzw. der Erstverschlüsselung entsprechen.

Die genannten Einschränkungen gelten für Serial ATA Festplatten nur dann, wenn sie als hot pluggable Festplatten genutzt werden.

- **Verschiedene Festplattentypen**
  Vermeiden Sie es wenn möglich, die unterschiedlichen Typen (IDE/SCSI) auf einem System zu mischen.

- **Unformatierte Bereiche**
  Wurde eine Partition keinem Dateisystem fest zugeordnet, wird dies von SafeGuard Easy beim Installationstyp „Bootschutz“ nicht erkannt, und es wird auch der unformatierte Teilbereich der Festplatte verschlüsselt.

- **Zusätzliche Festplatten**
  SafeGuard Easy erkennt automatisch, ob Ihr Rechner über eine oder mehrere Festplatten verfügt. Es sollten nach der Installation von SafeGuard Easy keine zusätzlichen Festplatten in das System integriert werden. Wollen Sie eine zusätzliche Festplatte in das System integrieren, sollten Sie zunächst SafeGuard Easy komplett entfernen. Nach der Deinstallation integrieren Sie die neue Festplatte und installieren das Programm.

- **Neupartitionierung**
  Wenn eine Festplatte neu partitioniert wurde, muss VOR der Installation von SafeGuard Easy ein Neustart durchgeführt werden. Bitte verändern Sie die Partitionierung der Festplatte nach der Verschlüsselung nicht mehr. Dies kann zu Datenverlusten führen.

- **Schlüssel**
  Es wird nur ein Festplattenschlüssel unabhängig von der Anzahl der Festplatten definiert.

- **Systemkernsicherung**
  Erstellen Sie nach der Festplattenverschlüsselung unbedingt eine Sicherung des Systemkerns!

11.3 Unterstützte Diskettenlaufwerke

SafeGuard Easy unterstützt jedes in einen Standard PC integrierte Laufwerk.

HINWEISE ZUR DISKETTENVERSCHLÜSSELUNG:

- **Boot-Diskette**
  Wenn die Diskettenverschlüsselung aktiviert ist, sollte in jedem Fall eine **verschlüsselte Boot-Diskette** erstellt werden.
- **Mehrere Diskettenlaufwerke**
  Ist mehr als ein Diskettenlaufwerk vorhanden, werden die verschiedenen Laufwerke nicht einzeln, sondern zusammengefasst („A+B“) angezeigt.

  Diskettenlaufwerke können nicht einzeln verschlüsselt werden.

  Der Verschlüsselungsstatus gilt für alle Diskettenlaufwerke.

11.4 Unterstützte Wechselmedienlaufwerke

- USB Speicherstick
- Speicherkarte in integriertem Lesegerät-Steckplatz (SD Karte, CF Karte etc.)
- Lenovo Microdrive
- USB ZIP Laufwerk
- Paralleles ZIP Laufwerk

HINWEISE ZUR WECHSELMEDIENVERSCHLÜSSELUNG:

- **Anschluss nach der Installation möglich**
  Wechselmedien müssen bei der Installation von SafeGuard Easy nicht angeschlossen sein (Ausnahmen sind möglich, wenn z.B. ein USB Speicherstick nicht mit dem Standard Microsoft Treiber zusammenarbeitet, sondern einen eigenen verlangt).

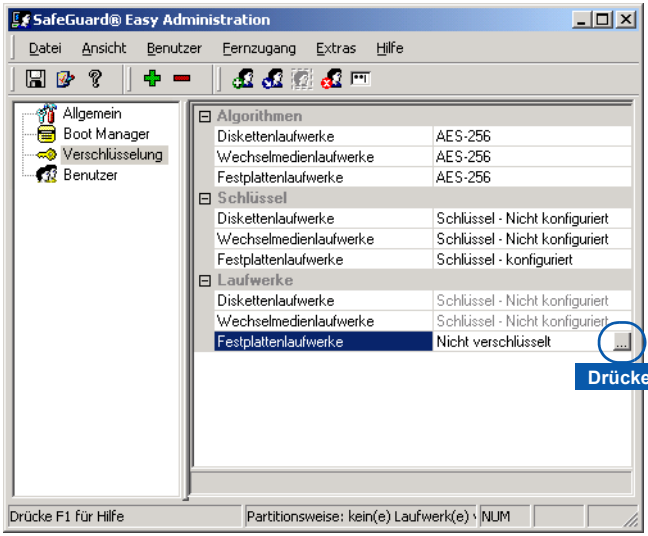
- **Erstverschlüsselung**
  Wechselmedien werden nicht „erstverschlüsselt“, sie werden formatiert sobald die Verschlüsselung eingeschaltet wird (jederzeit nach der Installation von SafeGuard Easy).

- **SG Eject**
  Wechselmedienlaufwerke werden wie Festplatten behandelt, sofern nicht entsprechende, vom Hersteller des Laufwerks stammende Software verwendet wird. Ist ein Wechselmedienlaufwerk verschlüsselt, können nur Benutzer mit Windows-Administratorrechten ein eingelegtes Medium auswerfen lassen. Benutzer ohne Administratorrechte müssen SG Eject benutzen. Zu finden ist SG Eject im Kontextmenü des Laufwerkes.

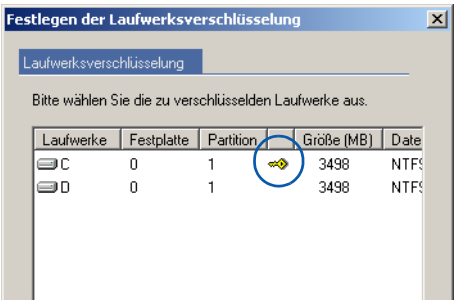
11.5 Laufwerke verschlüsseln

Im folgenden Beispiel verwenden wir die Festplattenverschlüsselung, für Disketten- und Wechselmedienlaufwerke ist die Vorgehensweise identisch:

1. Algorithmus für das Festplattenlaufwerk auswählen.
2. Schlüssel definieren.
3. Unter „Laufwerke“ auf „Festplattenlaufwerke“ doppelklicken.



4. Es öffnet sich der Dialog *Festlegen der Laufwerksverschlüsselung.*


Festlegen der Laufwerksverschlüsselung
Laufwerksverschlüsselung
Bitte wählen Sie die zu verschlüsselden Laufwerke aus.
Laufwerke Festplatte Partition Größe (MB) Date
C 0 1 3498 NTFS
D 0 1 3498 NTFS

Doppelklicken Sie auf einen Laufwerksbuchstaben, erscheint ein Schlüsselsymbol. Dadurch wird angezeigt, dass das Laufwerk / die Partition verschlüsselt wird.

Welche Festplatten bzw. wieviele Partitionen verschlüsselt werden (können), ist abhängig vom konfigurierten Verschlüsselungsmodus. Der Verschlüsselungsmodus (siehe 'Verschlüsselungsmodus') für eine Arbeitsstation wird während der Installation oder beim Erzeugen einer Konfigurationsdatei mit der Eigenschaft „Installieren“ gesetzt und ist im Nachhinein nicht mehr änderbar.

5. Wollen Sie die Verschlüsselung ausschalten, geschieht dies durch einen erneuten Doppelklick auf den Laufwerksbuchstaben. Das Schlüsselsymbol verschwindet und die Verschlüsselung ist deaktiviert.

11.6 Schlüssel

Nur ein Benutzer, der im Besitz des richtigen Schlüssels ist, kann auf verschlüsselte Laufwerke zugreifen. Ein Schlüssel besteht aus einer Aneinanderreihung von Ziffern (Zahlen, Buchstaben, bestimmte Sonderzeichen) und ähnlich wie ein Passwort unterliegt auch er bestimmten Regeln.

Laufwerks-Schlüssel müssen vor der Erstverschlüsselung vergeben werden. Sie können bei allen Laufwerken entweder selbst einen Schlüssel bestimmen oder sich vom System einen Zufallschlüssel generieren lassen.

11.6.1 Schlüsselmanagement

Das SafeGuard Easy Schlüsselmanagement speichert Schlüssel auf sichere Weise. Alle Schlüssel werden in einem verschlüsselten Bereich des SafeGuard Easy Systemkerns aufbewahrt und mit einem Verschlüsselungsschlüssel (dem sogenannten „KEK“ von **k**ey **e**ncryption **k**ey) verschlüsselt. Der KEK selbst ist nicht auf der Festplatte abgelegt, sondern wird aus dem SafeGuard Easy Passwort erzeugt.

11.6.2 Schlüsselerzeugung

Ohne korrektes Passwort sind die Schlüssel nicht zugänglich und demzufolge auch nicht die Daten auf Festplatte, Diskette oder Wechselmedium.

Ist die Pre-Boot Authentisierung eingeschaltet, werden die Schlüssel zum Entschlüsseln der Laufwerke nur erzeugt, wenn korrekte SafeGuard Easy-Zugangsdaten an der Pre-Boot Authentisierung eingegeben werden.

Ist die Pre-Boot Authentisierung ausgeschaltet, werden die Schlüssel einweg verschlüsselt und auf der Festplatte gespeichert.
Die Verschlüsselung und das Schlüsselmanagement ist trotzdem absolut identisch zur Auswahl 'Pre-Boot Authentisierung eingeschaltet'.
Die Handhabung des Passworts (bzw. des Scan Codes) allerdings nicht: Anstatt in der Pre-Boot Authentisierung darauf zu warten, dass ein Benutzer Benutzernamen und Passwort manuell eintippt, verfügt SafeGuard Easy über diese Daten. Dazu legt SafeGuard Easy - immer dann, wenn die Pre-Boot Authentisierung ausgeschaltet wird - einen Benutzer ('*AUTOUSER') an und kreiert für diesen ein Zufallspasswort. Dieses Passwort wird - in verschiedene Teile aufgeteilt - im SafeGuard Easy-Kern abgelegt. Beim Booten ist SafeGuard Easy in der Lage, daraus das komplette Passwort (oder eigentlich die komplette Scan Code Sequenz) wiederherzustellen.

11.6.3 Schlüssellänge

Für die Schlüssellänge gibt es keinen vorgegebenen Mindestwert, die maximale Zeichenanzahl beträgt allerdings 32 (32 bis 255 ASCII Code). Für den Schlüssel dürfen mit Ausnahme landesspezifischer Sonderzeichen alphanumerische Zeichen (A-Z; a-z; 0-9) und Sonderzeichen (°!“‘§$%&/()=?´*’-:;^+#-.,) verwendet werden. Beachten Sie, dass zwischen Groß- und Kleinschreibung unterschieden wird.

11.6.4 Triviale Schlüssel

Schlüssel für Disketten, Festplatten und Wechselmedien werden auf Trivialität überprüft. Unter einem trivialen Schlüssel werden Zeichenfolgen verstanden, die aus einem oder wenigen Zeichen bestehen (z.B. 22222222, aad daad daadd, 1h1h1h1h1h1h1h) oder die der Folge einer Tastaturreihe entsprechen (z.B. asdfghjk, lkjhgfds). Bei einem trivialen Schlüssel werden Sie auf das Sicherheitsrisiko hingewiesen und können einen neuen Schlüssel definieren.

11.6.5 Zufallsschlüssel

Ein Zufallsschlüssel hat immer die Länge von 32 Byte (256 Bit). Er wird dann auf die passende Länge des eingestellten Algorithmus reduziert. Die *-Zeichen im Eingabefeld für den Schlüssel dienen nur als Platzhalter.

Das Generieren eines Zufallsschlüssels für Festplatten bzw. Partitionen empfiehlt sich insbesondere bei der Installation von SafeGuard Easy auf mehreren Arbeitsstationen mit einer einzigen Konfigurationsdatei: Es werden hierbei trotz gleicher Konfigurationseinstellungen auf den jeweiligen Rechnern unterschiedliche, nicht triviale Zufallsschlüssel generiert.

Findet ein reger Austausch von Disketten/Wechselmedien bspw. unter Mitarbeitern statt, sollte der Schlüssel **nie** per Zufall generiert werden. Mit einem Zufallsschlüssel verschlüsselte Medien können nur auf der Arbeitsstation gelesen werden, auf der sie verschlüsselt wurden.

11.6.6 Schlüssel definieren

Alle Schlüssel können in der Grundeinstellung nur vom Administrator (SYSTEM) eingegeben werden. Anderen Benutzern muss das entsprechende Recht verliehen werden, damit auch diese die Möglichkeit haben. Schlüssel für Festplatte, Diskette und Wechselmedien können unterschiedlich sein. Für alle Laufwerke ist nur ein Schlüssel vergebbar.

Zur Erstvergabe oder Änderung eines Schlüssels klicken Sie auf den Unterpunkt „Schlüssel“. Die Eingabe des Schlüssels erfolgt für alle Laufwerke gleich. Es gelten auch die selben Schlüssel-Regeln.

Haben Sie den Schlüssel eingegeben bzw. wurde der Zufallsschlüssel gewählt, drücken Sie bitte zur Bestätigung die Schaltfläche [OK].

Geben Sie einen selbstgewählten Schlüssel nie an unbefugte Dritte weiter.

11.6.7 Schlüssel ändern

Verschlüsselte **Festplatte oder Partitionen** müssen zuerst entschlüsselt werden, bevor ein neuer Schlüssel gesetzt werden kann.

Der Schlüssel **für Disketten- und Wechselmedien** kann jederzeit entweder vom SafeGuard Easy-Benutzer SYSTEM oder von einem Benutzer mit entsprechenden Rechten neu gesetzt werden. Bitte beachten Sie aber, dass die mit dem „alten“ Schlüssel verschlüsselten Medien nicht mehr lesbar sind. Zugreifen können Benutzer auf „alte“ Medien nur, wenn sie über das Recht zum Schalten der Disketten-/ Wechselmedienschlüssel verfügen (siehe ’Disketten- und Geräteverschlüsselung schalten’).

11.7 Algorithmen

Gemessen werden die verschiedenen Algorithmen insbesondere an ihrer Sicherheit. Je sicherer ein Verfahren ist, desto länger dauert allerdings meistens der Verschlüsselungsprozess.

11.7.1 Algorithmus wählen

Um einen Algorithmus zu vergeben, klicken Sie unter *Algorithmen* auf ein Laufwerk und wählen im Pull-Down Menü einen Algorithmus aus.
Als Standard wird automatisch **AES-256** gewählt.

11.7.2 SafeGuard Easy Algorithmen

Im folgenden finden Sie eine Liste aller einsetzbaren Algorithmen mit ihren jeweiligen Standards:

Algorithmus	Schlüssellängen
AES-256	32 bytes (256 bits)
AES-128	16 bytes (128 bits)
Rijndael-256	32 bytes (256 bits)
DES	7 bytes (56 bits)
3DES	21 bytes (168 bits)
IDEA	16 bytes (128 bits)
Blowfish-8	32 bytes (256 bits)
Blowfish-16	32 bytes (256 bits)
STEALTH-40	6-8 bytes (48 - 64 bits)
XOR	8 bytes (64 bits)

AES-128
Der Advanced Encryption Standard (AES) ist ein Verschlüsselungsalgorithmus, welcher den DES Algorithmus ersetzt. Für diesen Algorithmus wurde vom National Institute for Standards and Technology (USA) der Algorithmus Rijndael ausgewählt. Es handelt sich dabei um einen sehr schnellen und sicheren Verschlüsselungsalgorithmus. AES-128 arbeitet mit einem 128-Bit-Schlüssel.

AES-256
Dieser Algorithmus entspricht dem AES-128 Algorithmus, arbeitet jedoch mit einem 256-Bit-Schlüssel und 128 bit Blocklänge.

Rijndael-256
Dieser Algorithmus ist eine spezifische Implementierung des AES-256. Er entspricht dem AES-256, verfügt jedoch über 256 bit Blocklänge.

IDEA
IDEA (International Data Encryption Algorithm) wurde Anfang der 90er Jahre entwickelt. Es ist ein symmetrischer Verschlüsselungsalgorithmus, der mit einem 128-Bit-Schlüssel arbeitet. Er wird heutzutage als sicher angesehen, sowohl in Bezug auf mathematische Verfahren als auch auf Schlüssellänge und gilt als äußerst resistent gegenüber allen Angriffen der Kryptoanalyse.

DES
DES (Data Encryption Standard) wurde in den 70er Jahren entwickelt und verwendet eine Schlüssellänge von 56 Bit.

3DES (Triple-DES)
Triple-DES, oder verkürzt 3DES, ist eine Weiterentwicklung des Data Encryption Standard (DES). 3DES verwendet drei aufeinanderfolgende Verschlüsselungsläufen des DES-Algorithmus und arbeitet mit einem 168-Bit-Schlüssel. Das 3DES-Verfahren gilt als sicher, ist aber etwas langsam.

Blowfish-16 / Blowfish-8
Blowfish ist ein symmetrischer Algorithmus. Er verwendet einen 64-Bit-Blockchiffrieralgorithmus und eine Schlüssellänge von 256 Bit.
Der Blowfish-8-Algorithmus entspricht dem Blowfish- 16-Algorithmus, ist jedoch auf acht Runden reduziert. Er verwendet eine Schlüssellänge von 256 Bit.

STEALTH-40
Dieser Algorithmus ist etwa gleich schnell wie XOR, aber deutlich sicherer. Der STEALTH-Algorithmus verwendet eine Schlüssellänge von 48-64 Bit.

XOR
XOR (eXclusive Or opeRation) ist ein symmetrischer Algorithmus und verwendet eine Schlüssellänge von 64 Bit. Seine Sicherheit ist allerdings als niedrig einzustufen.

HINWEIS:
Wenn Sie ein hochsicheres System aufsetzen wollen, verwenden Sie bitte IDEA oder AES/Rijndael.

Spezielle Algorithmen für Diskettenlaufwerke:

- **XOR SB-I A=B**
  Eigenschaften siehe XOR

  X SB-I A=B ist mit dem Diskettenchiffrierer von SafeBoard I (ab Version 1.43) C:Crypt und Crypton DOS kompatibel.

- **DES SB-II**
  Der Algorithmus DES SB-II ist kompatibel zur Diskettenverschlüsselung der SafeBoards II und III bzw. zu der Diskettenverschlüsselung der SafeBoards X II und III mit altem Schlüsselmanagement.

11.7.3 Algorithmus ändern

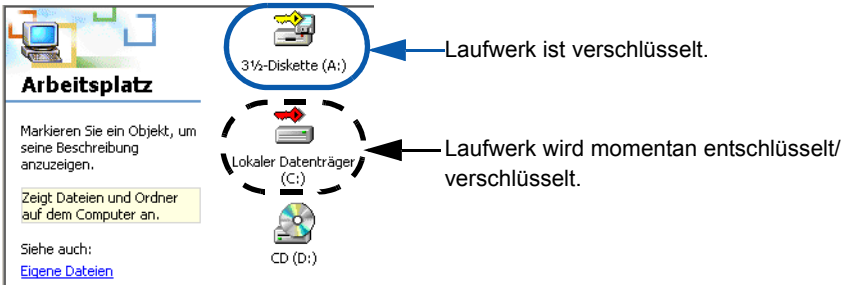
Sobald SafeGuard Easy installiert ist, können Algorithmen nicht mehr nachträglich geändert werden. Ein anderer Algorithmus erfordert eine Neuinstallation von SafeGuard Easy.

11.8 Verschlüsselungsstatus im Windows-Explorer anzeigen

Der Verschlüsselungszustand der Laufwerke wird im Windows Explorer mit einem farbigen Schlüssel markiert.

Gelber Schlüssel bedeutet, dass ein Laufwerk verschlüsselt ist.

Roter Schlüssel bedeutet, dass ein verschlüsseltes Laufwerk gerade entschlüsselt wird (oder umgekehrt).



11.9 Image einer verschlüsselten Festplatte erstellen

Images von Festplatten werden in Unternehmen in der Regel zur Erstinstallation einer großen Anzahl von PCs verwendet, wenn z.B. 10.000 Notebooks einer Versicherung unter Verwendung eines Image-Tools identisch aufgesetzt werden. Desweiteren dienen Image-Tools dazu, an einzelnen PCs beschädigte Partitionen per gespeicherter Image-Datei von CD/DVD zu restaurieren und das System wieder funktionsfähig zu machen.

In der Regel treten jedoch beim Erstellen von Images von verschlüsselten Festplatten (Partitionen) Probleme auf.

Gründe hier für sind:

- Ein Image einer verschlüsselten Partition kann niemals komprimiert werden. Dies bedeutet, dass ein Image einer verschlüsselten Partition immer genau so groß wird wie die tatsächliche Partition.
- Die Größe der verschlüsselten Partition darf sich nicht ändern. Ansonsten ist es nicht möglich, das Image zurückzuspielen.
- Wird eine mit SafeGuard Easy verschlüsselte Festplatte geklont, sind sämtliche zufällig erzeugte Verschlüsselungsschlüssel identisch.

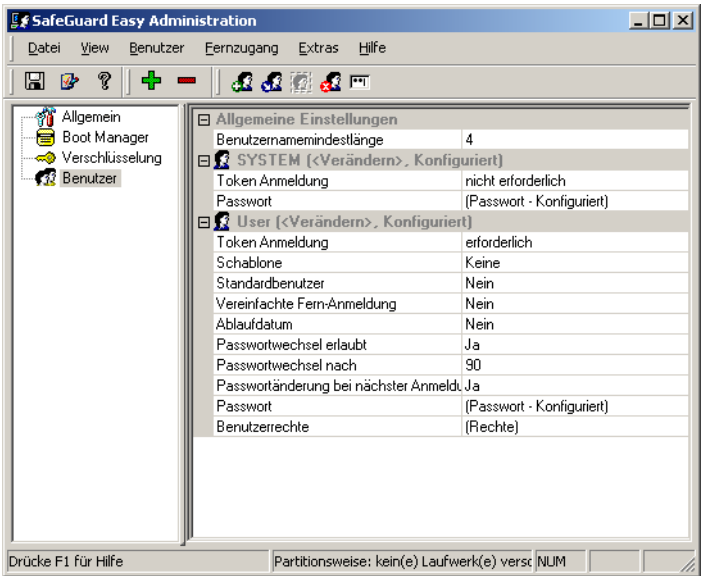
Es ist unter bestimmten Bedingungen trotzdem möglich, Festplattenpartitionen auf einer mit SafeGuard Easy verschlüsselten Festplatte mit Hilfe von Imaging-Software (z.B. Norton Ghost von Symantec) zu sichern und zu restaurieren.

Unter anderem muss das Image-Tool in die Lage versetzt werden, die verschlüsselte Partition zu entschlüsseln.

Weitere Informationen zu diesem Thema erhalten Sie in der Utimaco-Wissensdatenbank http://www.utimaco.de/myutimaco.

Nutzen Sie bitte die Suchfunktion der Wissensdatenbank, um nach Stichworten wie „Image“ oder „Imaging“ zu suchen.

12 Benutzerprofile erstellen



In diesem Bereich legen Sie fest, welche Benutzer an einem mit SafeGuard Easy geschützten Arbeitsplatz arbeiten dürfen. Sie können hier neue SafeGuard Easy-Benutzer anlegen, Bestehende modifizieren oder nicht benötigte Benutzer wieder entfernen. Außerdem bestimmen Sie, über welche zusätzlichen Eigenschaften und Rechte die definierten SafeGuard Easy-Benutzer verfügen.

SafeGuard Easy erlaubt maximal 16 Benutzern (inkl. *AUTOUSER) den Zugang zum System. Voreingestellt sind SYSTEM und USER wobei der Benutzer SYSTEM nie gelöscht werden darf.

HINWEIS:

Der Konfigurationsdateiassistent zeigt SYSTEM und USER nur an, wenn eine Datei mit der Eigenschaft „Installieren“ erzeugt bzw. als Basiskonfiguration verwendet wird.

12.1 Festlegen von Verwaltungsaufgaben

In SafeGuard Easy wird zwischen Benutzern mit Verwaltungsaufgaben und Benutzern ohne Verwaltungsaufgaben unterschieden.

Benutzer mit Verwaltungsaufgaben sind der

- Administrator und
- Benutzer mit Verwalterfunktionen

Die Person ohne Verwaltungsaufgaben ist der

- Benutzer.

Die Verwaltungsfunktion kann von der Benutzer-Funktion getrennt oder aber mit ihr vereint sein. Die Verwaltungsaufgaben können von einer oder mehr Personen erfüllt werden. SafeGuard Easy kann also für mindestens einen und maximal 16 Benutzer (inkl. *AUTOUSER)) konfiguriert werden.

Je nach Organisation kann es aber sinnvoll sein, ein mehrstufiges Rollensystem zu schaffen, wobei die Administratoren oder Unter-Systemverwalter unterschiedlich abgestufte Rechte erhalten. Folgende Hierarchiestruktur ist denkbar:

Administrator

Nur der Administrator kann alle Programm-Funktionen ausführen. Er kann einen Gehilfen definieren und diesem bestimmte Verwaltungsrechte verleihen. Der Administrator darf sein Passwort niemals vergessen. Er sollte es notieren und an einem sicheren Platz aufbewahren.

Unter-Systemverwalter

Unter-Systemverwalter können dem Benutzer weiterhelfen, wenn dieser z.B. sein Passwort vergessen haben sollte. Inwieweit ein Unter-Systemverwalter den Systemverwalter bei der Arbeit unterstützen kann, hängt von seinen vordefinierten Rechten ab.

Benutzer

Der Benutzer kann nur seine Einstellungen einsehen. Ausführen kann er aber standardmäßig nur die Funktion zur Benutzer-Passwort-Änderung. Zudem können ihm vom Administrator verschiedene Rechte gewährt werden.

12.2 Vordefinierte Benutzer

SafeGuard Easy stellt folgende, vordefinierte Benutzerprofile zur Verfügung:

- SYSTEM
- USER
- *AUTOUSER

12.2.1 Der Benutzer SYSTEM

Dieser Benutzer hat als einziger die höchste Hierarchiestufe. Er kann seine eigenen Einstellungen nicht ändern. Der Benutzer SYSTEM kann von niemandem gelöscht werden und ist von niemandem administrierbar. Der Benutzer SYSTEM kann als einziger die Einstellungen aller anderen Benutzerprofile ändern. Nur der oberste Sicherheitsbeauftragte des Systems sollte sich daher mit der Benutzerkennung SYSTEM anmelden können. Das Passwort für den Benutzer SYSTEM sollte also nur dem obersten Sicherheitsbeauftragten bekannt sein. Er sollte dieses Passwort notieren und z.B. in einem Tresor hinterlegen.

12.2.2 Der Benutzer USER

Wie der Benutzer SYSTEM ist der Benutzer USER nach einer SafeGuard Easy Installation automatisch vorhanden. Dieses Benutzerprofil verfügt über keinerlei Rechte und kann jederzeit gelöscht werden.

12.2.3 Der *AUTOUSER

Eine Besonderheit ist der *AUTOUSER. SafeGuard Easy legt immer wenn die Pre-Boot Authentisierung ausgeschaltet wird den *AUTOUSER an und kreiert für diesen ein Zufallspasswort. Dieses Passwort wird - in verschiedene Teile aufgeteilt - im SafeGuard Easy-Kern abgelegt. Beim Booten ist SafeGuard Easy in der Lage, daraus das komplette Passwort wiederherzustellen und die Anmeldung durchzuführen.

Der *AUTOUSER hat keine voreingestellten Rechte, allerdings können ihm die vier nachfolgend aufgeführten Rechte erteilt werden.

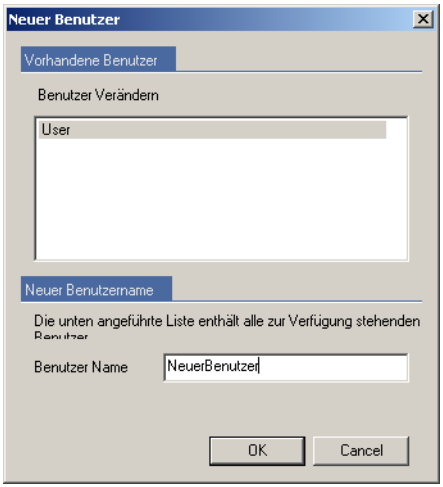
- Diskettenschlüssel temporär ändern
- Diskettenverschlüsselung schalten
- Wechselmedienschlüssel temporär ändern
- Wechselmedienverschlüsselung schalten

Bei ausgeschalteter Pre-Boot Authentisierung melden sich alle Anwender mit den dem *AUTOUSER zugewiesenen Rechten am System an. Wird die Pre-Boot Authentisierung wieder aktiviert, verschwindet der *AUTOUSER von der Benutzerliste.

12.3 Benutzer anlegen

Ein neues Benutzerprofil wird in den Verwaltungsprogrammen über die Konfigurationsseite „Benutzer“ angelegt.

Nach Drücken des Symbols für das Anlegen eines neuen Benutzers wird der Dialog *Neuer Benutzer* geöffnet.



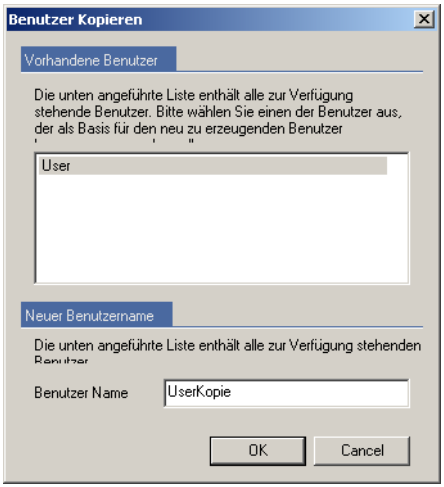
Geben Sie dem neuen Benutzer einen Namen, indem Sie eine Bezeichnung in das Eingabefeld eintragen. Der neue Benutzername darf **maximal 16 Zeichen** umfassen. Falls der Name schon vergeben ist, wird eine entsprechende Fehlermeldung ausgegeben.

Standardmäßig hat das neue Profil keine Rechte. Für die Verteilung von Rechten lesen Sie weiter bei Rechte zuweisen.

12.4 Benutzer kopieren

Benutzerprofile, die ähnlich sind, können Sie kopieren und dann ggf. ändern. Diese Vorgehensweise spart Zeit.

Nach Drücken des Symbols für das Kopieren eines neuen Benutzers wird der Dialog *Benutzer kopieren* angezeigt.


Benutzer Kopieren
Vorhandene Benutzer
Die unten angeführte Liste enthält alle zur Verfügung stehende Benutzer. Bitte wählen Sie einen der Benutzer aus, der als Basis für den neu zu erzeugenden Benutzer
User
Neuer Benutzername
Die unten angeführte Liste enthält alle zur Verfügung stehenden
Benutzer Name
UserKopie
OK
Cancel

Wählen Sie in der Benutzerliste das vorhandene Profil aus, das Sie kopieren wollen. Angezeigt werden alle Profile, die in Ihrem Verwaltungsbereich liegen. Sie können aber nur Profile kopieren, die eine niedrigere Hierarchiestufe aufweisen als Ihr eigenes Profil.

Der Benutzer SYSTEM kann nicht kopiert werden.

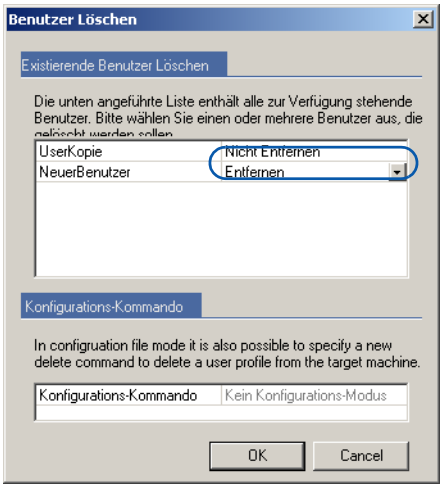
Geben Sie dem neuen Benutzer einen Namen und drücken Sie zur Bestätigung der korrekten Namensvergabe auf [OK]. Falls der Name schon vergeben ist, wird eine entsprechende Fehlermeldung ausgegeben.

Anschließend können Sie ggf. das neue Profil modifizieren.

12.5 Benutzer löschen

Benutzerprofile, die nicht mehr benötigt werden, können gelöscht werden.

Nach Drücken des Symbols für das Löschen eines Benutzers wird der Dialog *Benutzer löschen* angezeigt.


Benutzer Löschen
Existierende Benutzer Löschen
Die unten angeführte Liste enthält alle zur Verfügung stehende Benutzer. Bitte wählen Sie einen oder mehrere Benutzer aus, die
UserKopie
Nicht Entfernen
NeuerBenutzer
Entfernen
Konfigurations-Kommando
In configruation file mode it is also possible to specify a new delete command to delete a user profile from the target machine.
Konfigurations-Kommando
Kein Konfigurations-Modus
OK
Cancel

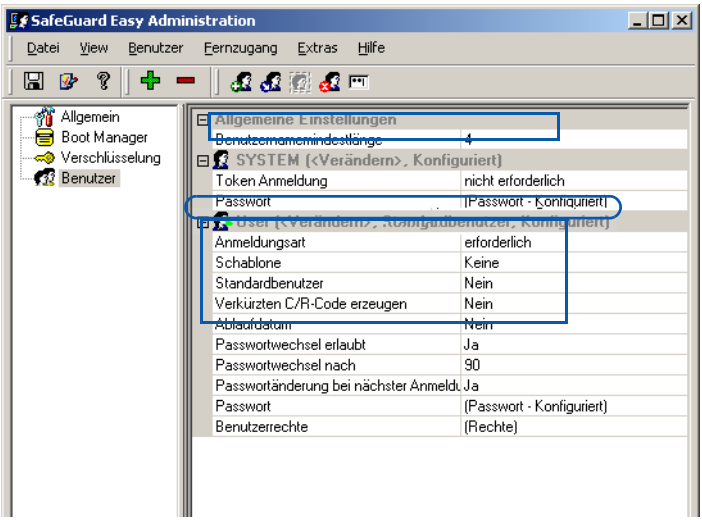
Wählen Sie in der Benutzerliste das vorhandene Benutzerprofil aus, das Sie löschen wollen. Angezeigt werden alle Profile, die in Ihrem Verwaltungsbereich liegen. Klappen Sie das Pull-Down Menü hinter dem Benutzernamen auf und ordnen Sie die Eigenschaft „Entfernen“ zu.

Sie können nur Benutzerprofile löschen, die eine niedrigere Hierarchiestufe aufweisen als Ihr eigenes Profil.

Das Entfernen eines Benutzers kann nicht mehr rückgängig gemacht werden.

12.6 Benutzermerkmale

Welches Merkmal einem Benutzer zugewiesen ist, erkennt man an den Erweiterungen hinter dem Benutzernamen.



12.6.1 Benutzernamenmindestlänge

In diesem Feld legen Sie fest, wieviele Zeichen ein Benutzername mindestens umfassen muss. Sie können den gewünschten Wert der Zeichen entweder direkt eingeben oder durch Betätigen der Richtungstasten vergrößern bzw. verkleinern. Es kann ein Wert zwischen einem und 16 Zeichen eingegeben werden.

12.6.2 Token-Anmeldung

Diese Einstellung legt fest, ob sich ein Benutzer mit Token anmelden muss oder nicht. Diese Option ist nur wählbar, wenn während der Installation die Token-Unterstützung mit der Option „Wahlweise“ installiert wurde. Details zur Token-Unterstützung lesen Sie unter 'Token-Unterstützung' nach.

12.6.3 Standardbenutzer

Ein Standardbenutzer meldet sich - sobald eine Authentisierung verlangt wird - nur mit seinem SafeGuard Easy-Passwort an. Alle andere Benutzer müssen sich mit Passwort und Benutzernamen, anmelden (siehe 'Erweiterte Anmeldung über die Taste [F2]').

Mit Ausnahme von SYSTEM kann jeder SafeGuard Easy-Benutzer als Standardbenutzer definiert werden.

12.6.4 Verkürzten C/R Code erzeugen

Diese Funktion eignet sich besonders für Unter-Systemverwalter, die für die Fernwartung per Challenge/Response zuständig sind. Die Eigenschaft „Verkürzten C/R Code erzeugen“ beeinflusst die Länge des Response Codes, der während eines Challenge/Response-Verfahrens ausgetauscht wird.

Benutzer mit der Eigenschaft „Verkürzten C/R Code erzeugen“ (und der Benutzer SYSTEM) erzeugen kurze Response Codes mit nur 30 Zeichen, während von „regulären“ SafeGuard Easy-Benutzern erzeugte Response Codes 56 Zeichen lang sind. Beim Eintippen bzw. Übermitteln an den Benutzer kann dies zu einer erhöhten Fehlerquote führen.

Einzelheiten über das Challenge/Response-Verfahren lesen Sie bitte im Kapitel 'Fernwartung (Challenge/Response)' nach.

12.6.5 Schablone

Schablonen erfüllen einen ganz besonderen Zweck: Sie dienen als Basisbenutzerprofil und werden i.d.R. dann eingesetzt, wenn SafeGuard Easy mit Hilfe einer Konfigurationsdatei auf mehreren Rechnern installiert werden soll. Gäbe es keine Schablonen, so würden die Benutzer auf allen Maschinen denselben Benutzernamen besitzen. Dies widerspricht jedoch in vielen Fällen den organisatorischen Richtlinien von Firmen, die besagen, dass es individuelle Benutzernamen/Passworte geben muss, z.B. Nachname, Personalnummer etc. Für solche Umgebungen kann dann ein SafeGuard Easy Benutzerprofil als Schablone definiert werden.

Das führt dazu, dass dieser SafeGuard Easy Benutzer bei der ersten Anmeldung in der Pre-Boot Authentisierung einen neuen Benutzernamen bekommt und somit individualisiert wird.

Eingesetzt wird die Schablonenfunktion folgendermaßen:

Der Administrator legt einen SafeGuard Easy Benutzer an und definiert diesen als Schablone. SafeGuard Easy wird dann mit diesen Einstellungen auf einem Zielrechner installiert. Dem Benutzer des Zielrechners werden Benutzername und Passwort des Benutzers, der als Schablone definiert wurde, für die erstmalige Anmeldung vom Administrator mitgeteilt. Meldet sich der Benutzer das erste Mal an, muss er diese Zugangsdaten am Anmeldebildschirm eingeben. Danach wird er aufgefordert, einen neuen Benutzernamen und ein neues Passwort einzugeben, mit dem er sich bei der nächsten Anmeldung auch identifizieren muss.

Eine Schablone kann entweder zum Umbenennen oder Kopieren eines Benutzers dienen.

Schablone umbenennen

Wollen Sie sicherstellen, dass sich nur genau ein Benutzer per Schablone an SafeGuard Easy anmeldet (bspw. bei mobilen Desktops für Außendienstmitarbeiter), weisen Sie der Schablone das Attribut „Umbenennen“ zu. Die Schablone wird mit den neuen Benutzerdaten überschrieben. Eine Anmeldung mit den bekannten Zugangsdaten ist nicht mehr möglich, da sie durch den angemeldeten Benutzer ersetzt wurden.

Schablone kopieren

Wird das Attribut „Kopieren“ gewählt, so wird der neue Benutzernamen zu den SafeGuard Easy-Benutzern hinzugefügt, aber die Schablone bleibt weiterhin bestehen. Weitere Benutzer können sich mit den Zugangsdaten der Schablone anmelden. Sind SYSTEM und USER voreingestellt, können noch maximal 13 Benutzer neu angelegt werden.

Aus Sicherheitsgründen wird empfohlen, die Schablonen nur zum „Umbenennen“ zu verwenden.

12.6.6 Ablaufdatum

Das Ablaufdatum bestimmt die maximale Gültigkeitsdauer für ein SafeGuard Easy Benutzerprofil. Sie können einen Stichtag (oder einen Zeitraum) festlegen, an dem der Benutzer sich letztmalig im System anmelden kann. Sie können das Datum bzw. die Zeitspanne durch Direkteingabe per Tastatur einstellen.

Geeignet ist diese Einstellung vor allem für den Fall, dass die Nutzung einer Arbeitsstation für Mitarbeiter nur für einen bestimmten Zeitraum vorgesehen ist, z.B. Ferienarbeiter oder Werkstudenten etc. Nach Ablauf der festgelegten Frist wird die Arbeitsstation für den Benutzer gesperrt.

Diese Einstellung hat keine Gültigkeit für den Benutzer SYSTEM.

12.7 Benutzerrechte

Überlegen Sie, welche Zugriffsberechtigungen den einzelnen SafeGuard Easy-Benutzer übertragen werden sollen. Die Vergabe der Rechte für die einzelnen Benutzer sollte aus Sicherheitsgründen gut durchdacht werden.

Sie können Benutzern Rechte für temporäre und permanente Einstellungen geben. Temporär heißt, bestimmte Einstellungen gelten nur für die Dauer einer Arbeitssitzung. Nach dem Neustart des Rechners sind sie nicht mehr gültig und die Systemeinstellungen werden wieder übernommen. Permanent sind Einstellungen, die auch nach einem Neustart noch vorhanden sind.

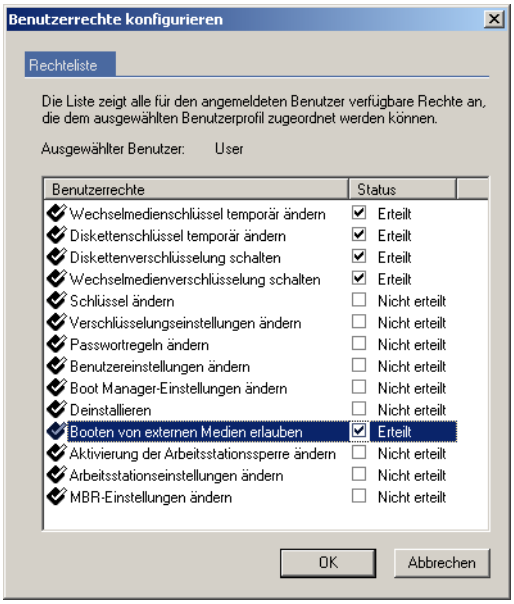
Folgende Rechte können vergeben werden:

Wechselmedienschlüssel temporär ändern	Erlaubt, den Schlüssel für Wechselmedienlaufwerke für die Dauer einer Anmeldung zu ändern.
Diskettenschlüssel temporär ändern	Erlaubt, den Schlüssel für Diskettenlaufwerke für die Dauer einer Anmeldung zu ändern.
Diskettenverschlüsselung schalten	Erlaubt, die Diskettenverschlüsselung ein- oder auszuschalten.
Wechselmedien-verschlüsselung schalten	Erlaubt, die Verschlüsselung von Wechselmedienlaufwerken ein- oder auszuschalten.
Schlüssel ändern	Erlaubt, die Schlüssel für alle Laufwerke zu ändern. Dies gilt nicht für die Festplatte, wenn diese verschlüsselt ist.
Verschlüsselungseinstellungen ändern	Erlaubt, Verschlüsselungsstatus und Schlüssel zu ändern
Passwortregeln ändern	Erlaubt, alle allgemeinen Passwortregeln zu ändern.

Benutzereinstellungen ändern	Erlaubt, alle Benutzereinstellungen zu ändern. Muss gesetzt sein, um anderen Benutzern Rechte zu verleihen!
Deinstallieren	Erlaubt, SafeGuard Easy zu deinstallieren.
Booten von externen Medien erlauben	Erlaubt, ein mit SafeGuard Easy geschütztes System von externen Medien wie Diskette oder CD zu starten.
Arbeitsstationseinstellungen ändern	Erlaubt, folgende allgemeine Einstellungen zu ändern: - Token - Wake On LAN - Passwort beim Systemstart ändern - Verdeckte Passworteingabe - Identifikation
MBR-Einstellungen ändern	Erlaubt, alle Einstellungen für den Master Boot Record zu ändern.
Bootmanager-Einstellungen ändern	Erlaubt, die Einstellungen des SafeGuard Easy Boot Managers zu ändern.

12.7.1 Benutzerrechte zuweisen

Nach einem Doppelklick auf „Benutzerrechte“ erscheinen alle vergebbaren Berechtigungen. Der Doppelklick auf ein Recht bewirkt, dass dessen Status je nach vorherigem Stand in „Erteilt“ bzw. „Nicht erteilt“ umgewandelt wird.



Alle neuen Benutzer besitzen zunächst keine Rechte, allein der Benutzer SYSTEM verfügt über alle Rechte. Rechte, zu deren Bearbeitung der Benutzer nicht befugt ist, sind in der Ansicht nicht dargestellt und können nicht geändert werden.

12.7.2 Benutzerrechte weitergeben

Ein Benutzer kann auch Rechte an andere Benutzer verteilen, selbstverständlich nur diese, über die er selbst verfügt. Möchte ein Administrator (z.B. Untersystemverwalter) seine eigenen Rechte ändern, kann er das nicht selbst tun. Er muss zu einem höherrangigen Administrator gehen und diesen um die gewünschten Änderungen bitten.

Um eigene Rechte an andere Benutzer weiterzugeben, muss ein Benutzerprofil mit dem Recht „Benutzereinstellungen ändern“ ausgestattet sein.

13 Passworteinstellungen

Das Passwort spielt eine zentrale Rolle in SafeGuard Easy. Aus dem an der Pre-Boot Authentisierung eingegebenen SafeGuard Easy-Passwort wird der zum Booten erforderliche Schlüssel zum Entschlüsseln einer verschlüsselten Festplatte berechnet.

Das SafeGuard Easy-Passwort sollte überlegt gewählt werden. Oft neigen jedoch Benutzer dazu, immer dieselben oder Passworte wie z.B. Vor- oder Nachnamen, Firmennamen, aneinandergereihte Buchstaben- oder Zahlenfolgen etc. zu verwenden. Leicht zu erratende SafeGuard Easy Passworte erleichtern unbefugten Dritten jedoch den Zugriff auf eine Arbeitsstation.

Wie konsequent man bzgl. der Vergabe von Passwortrestriktionen vorgehen möchte, sollte gut überlegt und auch getestet werden.

13.1 Vordefinierte Passwortregeln

Aus Sicherheitsgründen gibt SafeGuard Easy bestimmte Regeln für alle Benutzer-Passworte vor.

Ein SafeGuard Easy Passwort darf ...

- maximal 16 Zeichen haben.

Ein SafeGuard Easy-Passwort darf in keinem Fall...

- zu 50% (oder mehr) aus demselben Zeichen bestehen (z.B. aaabba, 222122).
- Zeichen und/oder Ziffern in Folge enthalten (z.B. abcdef, 1234567).
- Tastaturreihen enthalten (z.B. asdfghj).
- mit dem SafeGuard Easy-Benutzernamen identisch sein (Ausnahme: Passwort für den Benutzer „SYSTEM“).
- dem SafeGuard Easy-Benutzernamen ähnlich sein (Ausnahme: Passwort für den Benutzer „SYSTEM“).
- dem alten Passwort ähnlich sein.

Der Begriff „Ähnlich sein“ bedeutet hier, dass sich die Zeichenfolge des neuen Passworts in mindestens 20% vom alten Passwort / Benutzernamen unterscheiden muss.

BEISPIEL:

Der SafeGuard Easy-Benutzer „USER“ darf die Passworte „U2SER13“, „U345SER“ angeben, Passworte wie „USER1“, „USERa“, „USERab“, „12USER“, „1USERF“ lehnt SafeGuard Easy ab.

13.2 Erlaubte Tasten für das SafeGuard Easy-Passwort

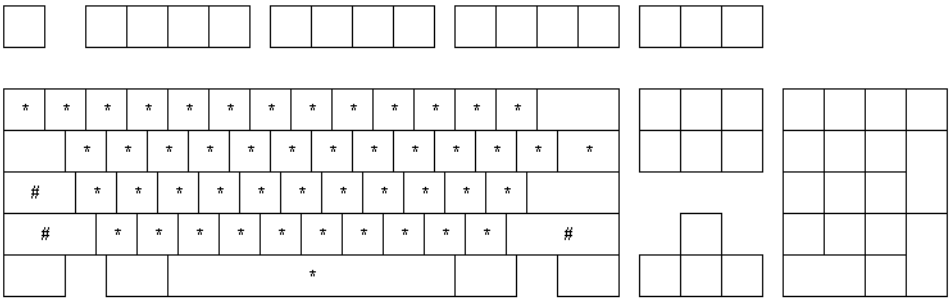
Das SafeGuard Easy-Passwort kann sich aus einer Mischung von alphanumerischen Zeichen und Satzzeichen zusammensetzen.

SafeGuard Easy akzeptiert

- alle Tasten, die in der Abbildung mit „*“ markiert sind.
- Die [Umschalt]-Taste und [Feststell]-Taste (in der Abbildung mit „#“ markiert).

SafeGuard Easy akzeptiert nicht

- die [Umschalt]-Taste, wenn die [Feststell]-Taste bereits aktiv ist.
- die [Alt]-Taste
- die [Strg]-Taste
- die Num-Tasten
- die F-Tasten (z.B. F1, F2)
- die Pfeil-Tasten



13.3 SafeGuard Easy für Einsatz im internationalen Umfeld konfigurieren

SafeGuard Easy speichert alle Zeichenabfolgen in „Scancode“-Form, da in der Pre-Boot-Phase in der Regel keine Tastaturtreiber geladen sind. Der Scancode ist eine Codenummer (Hexadezimaler ScanCode), welche die Tastatur bei einem Tastendruck an den PC weitergibt. Dieser Code ist unabhängig davon, welche Buchstaben, Ziffern oder Symbole auf der Taste abgebildet sind. Der Scan Code stellt ein spezielles Kennzeichen für die Taste selbst dar und ist für eine bestimmte Taste immer gleich.

13.3.1 Effekte verschiedener Tastaturlayouts

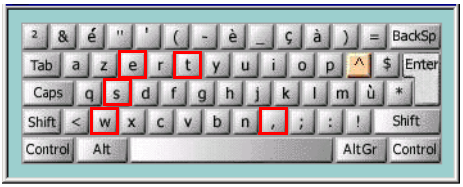
SafeGuard Easy speichert also Passworte als Scancodes. Das bedeutet, dass z.B. das Passwort „system“ bei **deutschem Tastaturlayout** als folgende Scancode-Sequenz gespeichert wird: 1f-2d-1f-14-12-32

„System“ auf einem **englischen Tastaturlayout** ergibt folgenden Scan Code: 1f-**15**-1f-14-12-32

Beachten Sie: Y und Z sind vertauscht! Der Benutzer müsste also „szstem“ eintippen, um sich erfolgreich zu authentisieren.

Auf einem **französischen Tastaturlayout** ergibt „system“ wieder einen anderen Scan Code, nämlich: 1f-**15**-1f-14-12-**27**.

Der Benutzer müsste „Swste,“ eintippen, um sich erfolgreich zu authentisieren.



Weitere Tastaturlayouts finden Sie unter

http://www.microsoft.com/globaldev/reference/keyboards.mspx

13.3.2 International einheitliche Zugangsdaten für SafeGuard Easy erzeugen

Sobald SafeGuard Easy in internationalen Umgebungen eingesetzt wird ist sicherzustellen, dass Passworte und Schlüssel auf allen verfügbaren Tastaturen korrekt eingegeben werden können. Auf weltweite Einsetzbarkeit sollte insbesondere bei den SafeGuard Easy Benutzerprofilen geachtet werden, die administrative Aufgaben erfüllen.

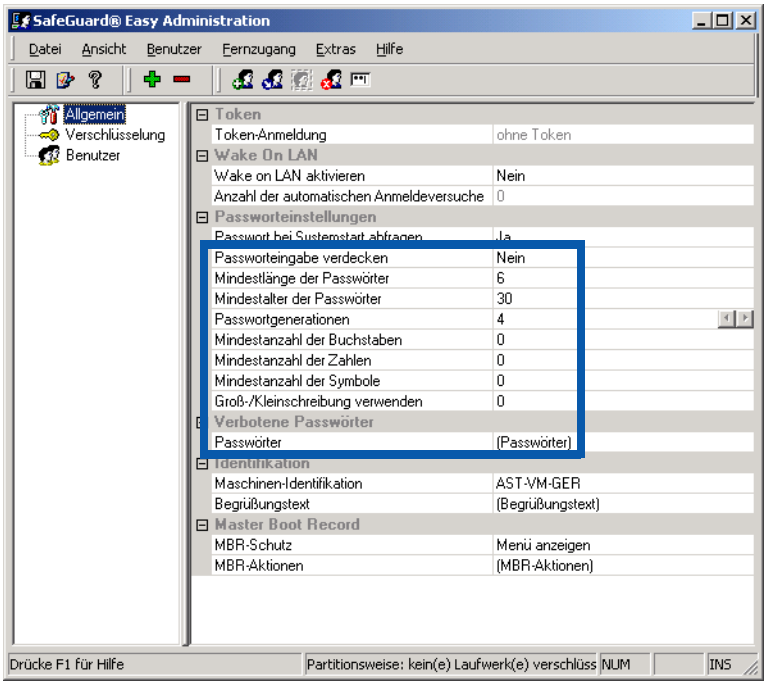
Als Beispiel zu nennen wäre das Challenge/Response-Verfahren, wenn der anrufende Benutzer und der Helpdesk-Benutzer, der den Response Code Assistenten bedient, unterschiedliche Tastaturlayouts benutzen.

Wenn die SafeGuard Easy-Zugangsdaten (besser: Tastenfolgen) aus einer Kombination der folgenden 21 Tasten erstellt werden, ist die Chance für einen problemlosen Einsatz von SafeGuard Easy in internationalem Umfeld sehr hoch.

Gedruckte Werte auf den Tasten	Hexadezimaler Scan Code
b	30
c	2E
d	20
e	12
f	21
g	22
h	23
i	17
j	24
k	25
l	26
n	31
o	18
p	19
r	13
s	1F
t	14
u	16
x	2D
v	2F
[Leerzeichen]	39

13.4 Allgemeine Passwortregeln

Die Allgemeinen Passworteinstellungen erlauben, weitere Vorgaben für die Zusammensetzung von SafeGuard Easy Passworten zu definieren, etwa den Anteil an Buchstaben und Zahlen oder deren Mindestlänge. Diese Vorgaben gelten für jeden SafeGuard Easy Benutzer, und es werden keine Passworte akzeptiert, die nicht diesen Standards entsprechen.



13.4.1 Passworteingabe beim Systemstart abfragen

Siehe 'Passwort beim Systemstart abfragen'.

13.4.2 Passworteingabe verdecken

Bei der verdeckten Passworteingabe werden im Gegensatz zu herkömmlichen Anmeldeprozeduren bei Eingabe des SafeGuard Easy Passworts keine Platzhalter (z.B. ´*´-Symbole) angezeigt. Ist diese Option aktiviert, ist auch die Cursor-Bewegung deaktiviert.

Bitte machen Sie Ihre Benutzer darauf aufmerksam, dass bei einem Tastendruck keine Zeichen angezeigt werden!

13.4.3 Mindestlänge der Passwörter

In diesem Feld legen Sie fest, wieviele Zeichen ein Passwort bei der Änderung durch den Benutzer mindestens umfassen muss. Sie können den gewünschten Wert der Zeichen entweder direkt eingeben oder durch Betätigen der Richtungstasten vergrößern bzw. verkleinern. Es kann ein Wert zwischen einem und 16 Zeichen eingegeben werden.

13.4.4 Mindestalter der Passwörter

Das Passwortalter gibt eine Mindestdauer in Tagen an. Innerhalb dieses Zeitraums darf der Benutzer das Passwort nicht ändern. Diese Option verhindert, dass sich der Benutzer das ursprüngliche Passwort wieder zurücksetzen kann.

13.4.5 Passwortgenerationen

Um zu verhindern, dass der Benutzer ständig zwischen wenigen Passwörtern wechselt, können Sie die Anzahl der Passwortgenerationen höher ansetzen. Jedes Passwort wird mit den in der Vergangenheit benutzten verglichen und bei Übereinstimmung mit einem bereits Verwendeten abgelehnt. Wieviele in der Vergangenheit benutzte Passworte zum Vergleich gespeichert werden, regelt diese Einstellung.

Die maximale Anzahl der speicherbaren, bereits verwendeten Passworte beträgt 16. Sie können den Wert sowohl nach einem Klick in das Eingabefeld über die Tastatur eingeben als auch mit Hilfe der Richtungspfeile verändern. Sinnvoll ist die Definition von Passwortgenerationen insbesondere in Verbindung mit der Einstellung „Passwortwechsel nach ´n´ Tagen“ (siehe ’Passwortwechsel nach (´n´ Tagen)’).

BEISPIEL:

Die Anzahl der Passwortgenerationen für den Benutzer Müller wurde auf 4 festgelegt, die der Tage, nach denen der Benutzer das Passwort wechseln muss, auf 30. Herr Müller meldete sich bislang mit dem SafeGuard Easy-Passwort „Informatik“ an. Nach Ablauf der Frist wird er im SafeGuard Easy-Anmeldebildschirm aufgefordert, sein Passwort zu ändern. Herr Müller tippt wieder „Informatik“ ein und erhält die Fehlermeldung, dass er dieses Passwort bereits verwendet hat und ein anderes Passwort wählen muss. „Informatik“ darf Herr Müller erst nach der vierten (da Passwortgenerationen = 4) Aufforderung zur Eingabe eines neuen Passworts wieder verwenden.

13.4.6 Mindestanzahl an Buchstaben, Zahlen, Symbolen

Um die Sicherheit von Passworten zu erhöhen, können Sie eine Mischung von Buchstaben und Zahlen (und/oder Symbolen) verlangen. Die angegebene Zahl setzt immer einen Mindestwert.

Symbole sind Zeichen wie * # !“§$%&/() etc.

13.4.7 Groß-/Kleinschreibung verwenden

Groß-/Kleinschreibung bedeutet, dass genausoviele Groß- wie Kleinbuchstaben verwendet werden müssen.

Das folgende **Beispiel** zeigt den korrekten Einsatz von Syntaxregeln:

Vorgabe:

Mindestanzahl der Buchstaben: 1
Mindestanzahl der Zahlen: 2
Mindestanzahl der Symbole:1
Groß-/Kleinschreibung verwenden: 2

Ergebnis:

- AAaa12# darf verwendet werden
- aaAA123## darf verwendet werden
- 3456## wird abgelehnt
- AAB1# wird abgelehnt

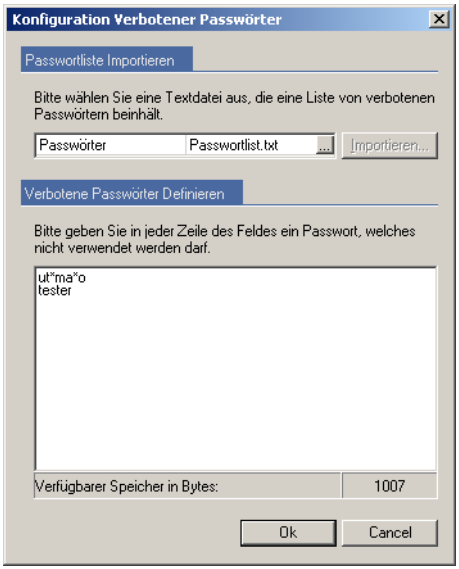
Bereits bestehende Kennwörter von Benutzern gelten weiterhin, auch wenn sie nicht mehr den Vorgaben entsprechen. Die Regeln greifen erst, wenn der Benutzer sein Passwort ändert.

13.5 Verbotene Passworte

Verbotene Passworte definieren bestimmte Zeichenfolgen, deren Verwendung im SafeGuard Easy Passwort ausgeschlossen ist. Jedes neue Passwort wird gegen die Liste verglichen und nur angenommen, wenn es nicht enthalten ist. Sie können eine bereits bestehende Liste importieren oder verbotene Passworte selbst eintragen.

13.5.1 Verbotene Passworte definieren

Doppelklicken Sie auf „Passwörter“, geben Sie unter „Verbotene Passwörter definieren“ nicht erlaubte Ziffernkombinationen ein und trennen Sie sie mit STRG + Eingabe.



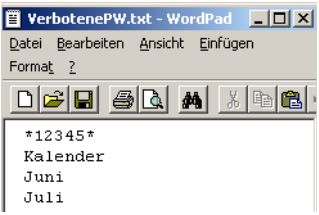
In die Liste sollten triviale Passworte wie Test, System, Benutzer usw. eingetragen werden. Alle Passworte, die einem verbotenen Passwort ähnlich sind, werden abgelehnt. Der Begriff „Ähnlich sein“ bedeutet hier, dass sich die Zeichenfolge des Passworts in mindestens 20% vom verbotenen Passwort unterscheiden muss. Steht bspw. „tester“ in der Liste, darf der Benutzer als Passwort „tester1234“ angeben, „tester12“ lehnt SafeGuard Easy ab.

Sie können auch Wildcards einsetzen. Als Wildcardzeichen wird nur das *-Symbol akzeptiert. Das Zeichen „*“ steht für **ein** beliebiges Zeichen im Passwort. Beispielsweise werden durch „ut*ma*o“ Passworte wie „utimaco“, „ut1ma2o“ etc. verboten.

ACHTUNG:
Wenn Sie nur die Wildcard oder entsprechend viele Wildcards in die Liste verbotener Kennwörter einfügen, können sich Benutzer nach einer erzwungenen Passwortänderung nicht mehr im System anmelden.

13.5.2 Passwortliste importieren

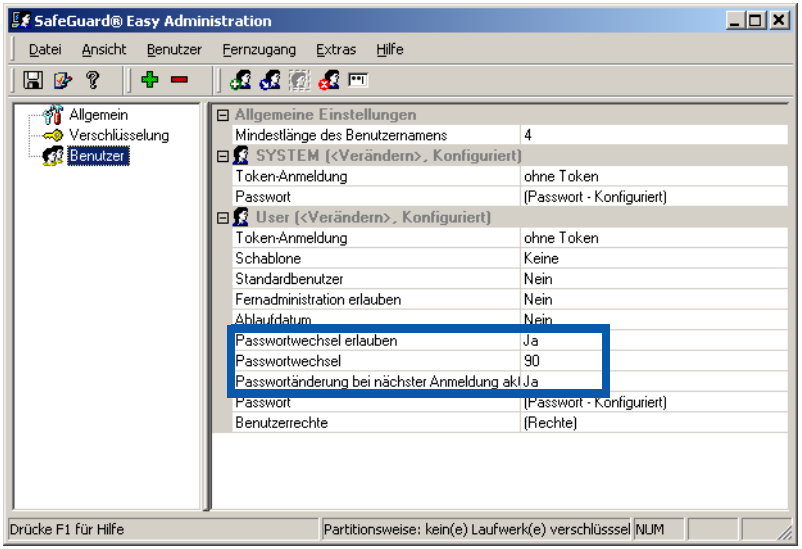
Ist bereits eine Liste mit verbotenen Passworten vorhanden, kann diese importiert werden. Dadurch können Sie an mehreren Arbeitsstationen die selbe Liste verwenden. Die Liste wird mit einem beliebigen Editor erstellt und könnte folgendermaßen aussehen:



Getrennt werden die unterschiedlichen Passworte mit einem Leerzeichen oder durch einen neuen Zeilenanfang.

HINWEIS:
Benutzer dürfen auf diese Datei keinen Zugriff haben!

13.6 Benutzerspezifische Passwortregeln



Die benutzerspezifischen Passwortregeln befassen sich mit Optionen für den Passwortwechsel.

13.6.1 Passwortwechsel erlauben

Diese Option steuert, ob ein Benutzer sein SafeGuard Easy-Passwort in der Pre-Boot Authentisierung oder Administration ändern darf oder nicht.

13.6.2 Passwortwechsel nach (´n´ Tagen)

Ein SafeGuard Easy-Passwort ist unbegrenzte Zeit gültig. Allerdings ist die Gefahr, dass es bekannt wird, sehr groß. Um das Sicherheitsrisiko zu minimieren, können Sie festlegen, dass ein Benutzer sein Passwort nach einer festgelegten Anzahl von Tagen ändern muss.

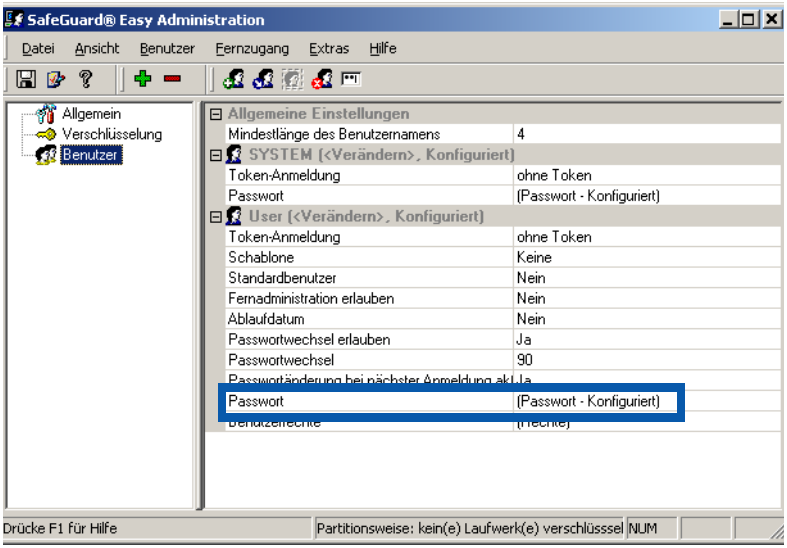
Stellen Sie die Zeitspanne, nach der das Passwort geändert werden muss, mit Hilfe der Richtungstasten oder über direkte Eingabe per Tastatur ein.

Der Zeitraum für die Gültigkeit der Passworte kann zwischen 1 und 365 Tagen liegen. Die Standardvorgabe beträgt 90 Tage. Ist die Frist abgelaufen, muss der Benutzer bei der nächsten Anmeldung sein Passwort ändern.

13.6.3 Passwortänderung bei nächster Anmeldung

Der Benutzer muss sein SafeGuard Easy-Passwort bei der nächsten Anmeldung ändern. Um die Funktion zu nutzen, muss die Pre-Boot Authentisierung aktiviert sein.

13.7 Passwort definieren



Benutzerpasswörter sollten überlegt gewählt werden, damit sie nicht einfach ausgespäht werden können. Sie dürfen sämtliche Buchstaben (Groß- oder Kleinschreibung), Ziffern und Zeichen (!“§$%&/()*+;,:._-) enthalten - soweit die Zusammensetzung nicht durch die Allgemeinen Passwortregeln eingeschränkt wurde.

Das Benutzerpasswort darf maximal 16 Zeichen umfassen!

Die Zahlen des Zahlenblocks dürfen nicht verwendet werden.

Doppelklicken Sie auf „Passwort“, erscheint der Dialog, in dem das Passwort definiert wird.

Geben Sie in die obere Zeile das gewünschte Passwort ein und tragen Sie es erneut in das Feld Bestätigung ein. Die Wiederholung ist notwendig, da Tippfehler vermieden werden sollen. Die Gleichheit der eingegebenen Zeichen wird geprüft und eine Fehlermeldung ausgegeben, falls die Passworte nicht übereinstimmen oder trivial (bspw. „12345“ oder „AAABBB“) sind. Aus Sicherheitsgründen wird der Eintrag nur mit ´*´-Symbolen angezeigt. Zur Korrektur von Einträgen verwenden Sie bitte die Rückstelltaste.

Das Umgehen der nochmaligen Passworteingabe durch das „Kopieren und Einfügen“ - Verfahren ist nicht möglich.

14 Twinboot/Bootmanager

Twinboot ist eine Installationsvariante, die es Ihnen erlaubt, eine klare Trennung zwischen geschäftlichem und privatem Bereich eines PCs vorzunehmen.

14.1 Funktionsweise

Twinboot verlangt für den Schutz von vertraulichen Geschäftsdaten zwei primäre Partitionen mit jeweils einem bootfähigen Betriebssystem. Twinboot verschlüsselt eine Partition (Geschäftspartition), während die andere im Klartext bleibt (Privatpartition). Die Geschäftspartition ist nur zugänglich mit dem SafeGuard Easy Passwort. Im Privatbereich besteht dagegen kein Schutz durch SafeGuard Easy, die Daten sind unverschlüsselt.
Geschäfts- und Privatbereich sind füreinander unsichtbar, es können also keine sensiblen Daten von der Geschäftspartition auf die ungeschützte Privatpartition transferiert werden. Wenn der Datenaustausch zwischen verschlüsselter und unverschlüsselter Partition gewünscht ist, macht dies eine Option möglich.

Über den **SafeGuard Easy Bootmanager** entscheiden Sie beim Starten des Rechners, welche Partition (Privat/Geschäftlich) gebootet wird. Ein Bootmanager-Menü erscheint auf dem Bildschirm und zeigt die verschiedenen Betriebssysteme an. Die verschlüsselte Partition verlangt die Authentisierung mit dem SafeGuard Easy-Passwort in der Pre-Boot Authentisierung, während für die unverschlüsselte Partition keine Authentisierung erforderlich ist. Aus diesem Grund muss die Entscheidung, welches Betriebssystem gestartet wird, vor der (möglichen) Pre-Boot Authentisierung fallen.

Die Twinboot Installation verlangt die Aktivierung von **Disketten- und Wechselmedienverschlüsselung** (ZIP-, MO-Laufwerke). Disketten und Wechselmedien bleiben verschlüsselt, sobald man den PC von der verschlüsselten (Geschäfts) Partition startet. Wird die Klartext (Privat) Partition gewählt, sind Disketten- und Wechselmedienlaufwerke unverschlüsselt, können aber von SafeGuard Easy-Benutzern mit den entsprechenden Benutzerrechten temporär aus-/eingeschaltet werden.

HINWEIS:
Weitere auf dem PC/Notebook vorhandene Partitionen können verschlüsselt werden oder unverschlüsselt bleiben.

14.2 Voraussetzungen

- Eine Twinboot-Installation ist nur erlaubt, wenn **eine einzige Festplatte** angeschlossen ist. Werden zwei Festplatten erkannt, ist die Twinboot Option ausgegraut. Weitere Festplatten können erst nach der Twinboot-Installation angeschlossen werden, es wird allerdings keine SafeGuard Easy-Unterstützung in Form von Verschlüsselung für diese zusätzliche Festplatte gewährleistet.
- Auf der vorhandenen Festplatte müssen vor der Installation von SafeGuard Easy **mindestens zwei primäre Partitionen** mit jeweils einem bootfähigen Betriebssystem existieren.
- VOR der Installation von SafeGuard Easy sollten alle Betriebssysteme (**nur Windows wird unterstützt**!) installiert und die Partitionierung der Festplatte festgelegt sein. Nachträgliche Änderungen werden nicht empfohlen.

14.3 Beispiel

Ausgangskonfiguration

C:\	D:\	E:\	F:\	G:\
primäre Partition	primäre Partition	logisches LW in erweiterter Partition	logisches LW in erweiterter Partition	logisches LW in erweiterter Partition
verschlüsselt	unverschlüsselt	verschlüsselt	unverschlüsselt	unverschlüsselt
Bootlaufwerk 1	Bootlaufwerk 2			

Start des verschlüsselten Bootlaufwerks 1

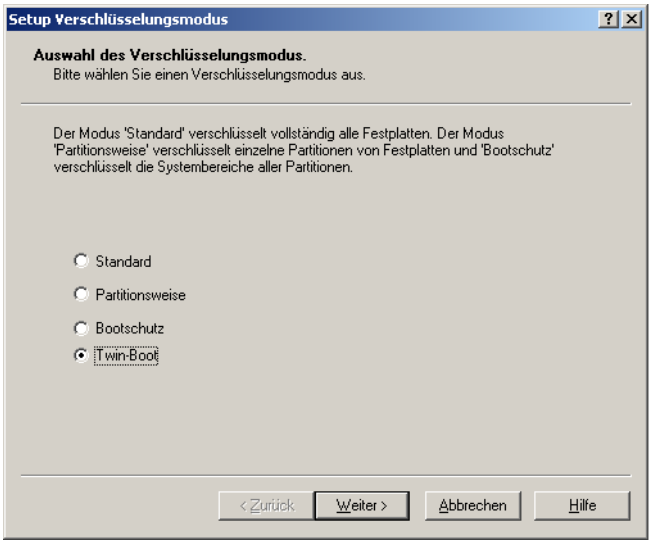
C:\	D:\	E:\	F:\	
primäre Partition	logisches LW in erweiterter Partition	logisches LW in erweiterter Partition	logisches LW in erweiterter Partition	
verschlüsselt	verschlüsselt	unverschlüsselt	unverschlüsselt	unverschlüsselt
Bootlaufwerk 1				Bootlaufwerk 2
lesbar	lesbar	*nicht lesbar*	*nicht lesbar*	*unsichtbar*

Start des unverschlüsselten Bootlaufwerks 2

C:\	D:\	E:\	F:\	
primäre Partition	logisches LW in erweiterter Partition	logisches LW in erweiterter Partition	logisches LW in erweiterter Partition	
unverschlüsselt	verschlüsselt	unverschlüsselt	unverschlüsselt	verschlüsselt
Bootlaufwerk 2				Bootlaufwerk 1
lesbar	*nicht lesbar*	lesbar	lesbar	*unsichtbar*

14.4 Twinboot konfigurieren

1. Erstellen Sie zwei primäre Partitionen und installieren Sie auf jeder Partition ein bootfähiges Betriebssystem.
2. Booten Sie anschließend die Partition, die als „Geschäftspartition“ dienen soll.
3. Starten Sie die lokale Installation von SafeGuard Easy.
   Bestätigen Sie in der Folge alle Eingaben mit [Weiter].
4. Im Dialog „Verschlüsselungsmodus“ markieren Sie „Twinboot“.



5. Wählen Sie in den SafeGuard Easy Verwaltungsprogrammen den Ordner **Verschlüsselung**. Neben der in der Grundeinstellung bereits als verschlüsselt markierten „Geschäftspartition“ (=Primäre Partition, die die zum Booten benötigten Dateien wie Ntldr, Boot.ini, Ntdetect.com enthält) müssen folgende Laufwerke verschlüsselt werden:

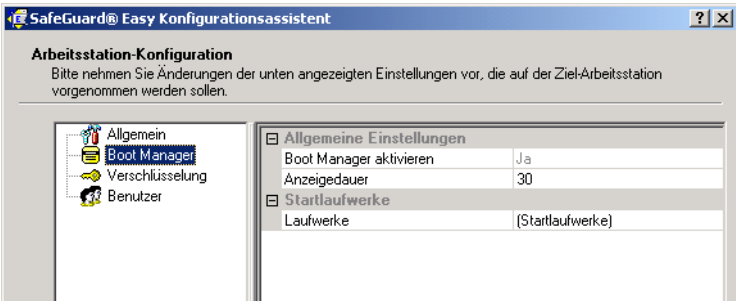
   - das Windows Systemlaufwerk, auf dem sich die Windows Systemdateien befinden (kann identisch sein mit der Bootpartition).
   - das Laufwerk mit dem SafeGuard Easy-Installationsverzeichnis, um den Zugriff auf die SafeGuard Easy-Dateien zu gewährleisten.
   - Eine Twinboot Installation verlangt zusätzlich, dass Disketten- und Wechselmedienlaufwerke verschlüsselt werden.

6. Der Twinboot Modus aktiviert automatisch den SafeGuard Easy Bootmanager. Wechseln Sie zum Ordner „Boot Manager“ und nehmen Sie die Feineinstellungen vor.

HINWEIS:
Beim Anwählen von Partitionen, auf die der Zugriff verboten ist, erscheint nach der Installation ein Dialog mit „Wollen Sie Partition formatieren“. Wenn Sie [JA] drücken, sind die Daten verloren!

14.5 Bootmanager konfigurieren

Konfiguriert wird der Bootmanager über den gleichnamigen Ordner in den Verwaltungsprogrammen. Die Konfigurationsseite wird aber nur bei Wahl des Verschlüsselungsmodus „Twinboot“ angezeigt.



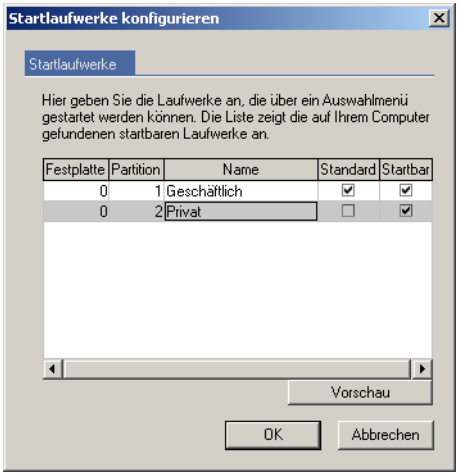
14.5.1 Allgemeine Einstellungen

- **Bootmanager aktiviert:**
  Definiert, ob der Bootmanager ein-/ausgeschaltet ist. Bei einer Twinboot Installation ist er in der Grundeinstellung eingeschaltet.

- **Anzeigedauer (Standard: 30)**
  Das Bootlaufwerk mit der Eigenschaft „Standard“ (festzulegen unter „Startlaufwerke“) startet beim Systemstart automatisch, wenn sich der Benutzer innerhalb eines bestimmten Zeitraums nicht für ein anderes Bootlaufwerk entscheidet. Diese Zeitspanne wird über das Feld „Timeout“ definiert. Gibt es kein Standardlaufwerk, startet das Betriebssystem der ersten primären Partition.

14.5.2 Startlaufwerke

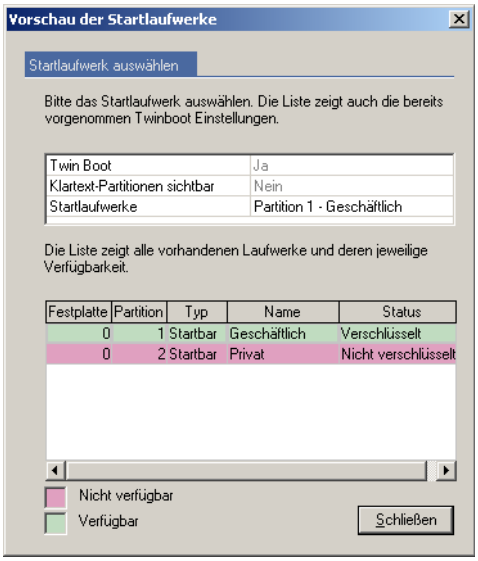
Nach einem Doppelklick auf Startlaufwerke wird der gleichnamige Dialog geöffnet. Hier werden die Eigenschaften des Bootmanager-Menüs definiert.



Es wird eine Liste angezeigt, die alle **primären Partitionen** des Rechners darstellt.

Zur Unterscheidung der verschiedenen bootfähigen Laufwerke im Bootmanager-Menü empfiehlt es sich zunächst, „sprechende“ **Bootnamen** einzutragen (maximal 40 Zeichen, z.B. „Privat“). Die eingetragenen Namen werden später im Auswahlmenü des Bootmanagers angezeigt. Damit ein Laufwerk im SafeGuard Easy-Bootmanager angezeigt wird, muss es als „**startbar**“ markiert werden. Eines der angezeigten Laufwerke muss zudem zum **Standardlaufwerk** gemacht werden, das automatisch beim Systemstart aufgerufen wird, wenn keine Auswahl im Bootmanager erfolgt.

Über die **Vorschau** lassen sich Verschlüsselungsstadium und Zugriff getrennt nach gewählter Bootpartition anzeigen.



Twin-Boot:
Zeigt, ob dieser Verschlüsselungsmodus aktiv ist.

Klartext-Partitionen sichtbar (wird eingestellt unter Verschlüsselung / Twinboot / Zugriff auf unverschlüsselte Laufwerke):
Zeigt, ob Datenaustausch zwischen verschlüsselten und unverschlüsselten Partitionen möglich ist.

Startlaufwerk:
Zeigt die Zugriffsberechtigungen abhängig vom Startlaufwerk, hat aber KEINE Auswirkung auf die unter „Startlaufwerke festlegen“ getroffenen Einstellungen.

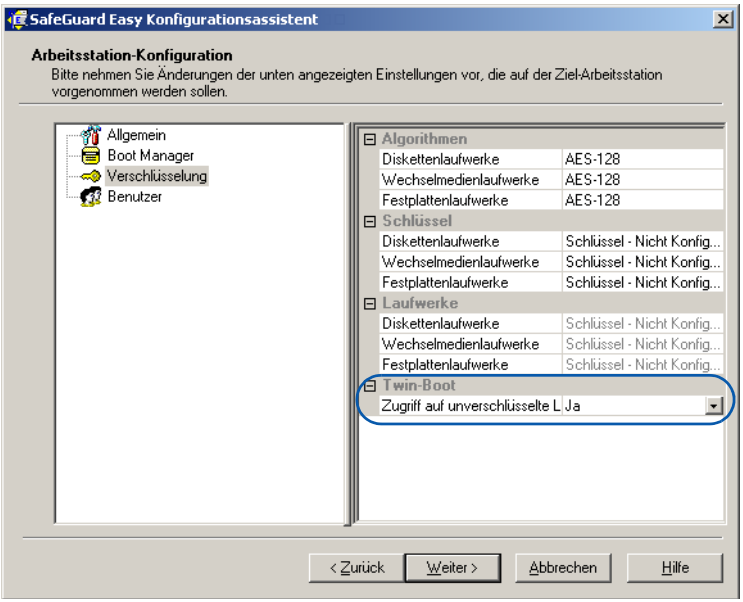
HINWEISE:

- Aus technischen Gründen funktioniert der Bootmanager erst, wenn Verschlüsselungs-/Entschlüsselungsprozesse abgeschlossen sind. Der erste Neustart nach Ver-/Entschlüsselung ruft automatisch das Betriebssystem des Windows Systemlaufwerks auf ohne den Bootmanager zu starten. Dieses Verhalten tritt insbesondere bei einer Twinboot Installation und nach Erzeugen eines Kernelbackups mit dem Assistenten für die Notfalldiskette auf.
- Der Bootmanager ändert für jede bootfähige primäre Partition, die nicht gestartet wurde, den Eintrag für den Partitionstyp in der Partitionstabelle auf „Hidden (48h)“. Auch wenn der SafeGuard Easy MBR Bootcode mit dem Kommando FDISK / MBR entfernt werden soll, bleiben diese Änderungen erhalten.

  Grundsätzlich ist FDISK /MBR mit großer Vorsicht zu verwenden. Um den Partitionstyp wiederherzustellen, müssen Sie SafeGuard Easy deinstallieren!

14.6 Daten zwischen Bootpartitionen austauschen

Sollte aus bestimmten Gründen der Datenaustausch zwischen Geschäfts- und Privatpartitionen nötig sein, ermöglicht dies die Einstellung „**Zugriff auf unverschlüsselte Laufwerke**“ in den Verschlüsselungseinstellungen.



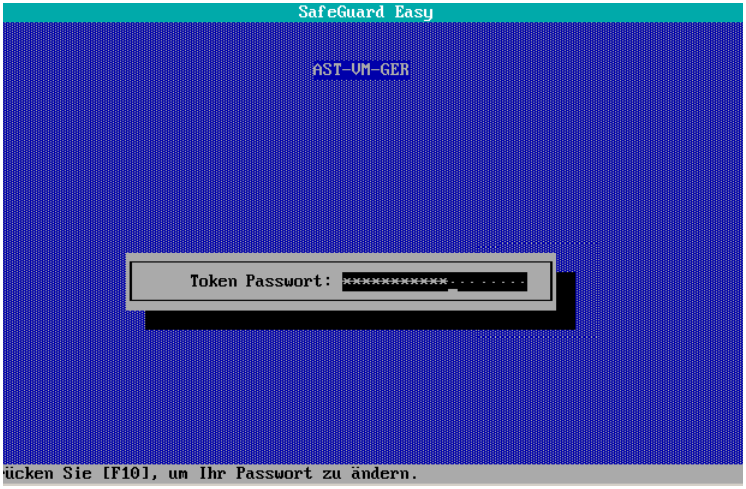
Steht diese Einstellung auf „JA“, ist der Zugriff auf unverschlüsselte Partitionen möglich, auch wenn die verschlüsselte Partition gestartet wurde.

Der Benutzer benötigt zum Ändern der Einstellung das Recht „Verschlüsselungseinstellungen ändern“.

15 Token-Unterstützung

Die Authentisierung mit Benutzername und Passwort genügt heutzutage oft nicht mehr den Kundenanforderungen nach optimalem Schutz vor Angriffen von Dritten. Deswegen bietet SafeGuard Easy als Alternative zur „traditionellen“ Anmeldemethode und zur Steigerung der Sicherheit die Anmeldung mit USB Token. Die Token-Anmeldung basiert auf dem Prinzip der Zwei-Faktor-Authentisierung: Ein Benutzer verfügt über einen Token (Besitz), kann den Token aber nur nutzen, wenn er das spezifische Token-Passwort kennt (Wissen).

Im Anwendungsfall steckt der Benutzer einen Token in die USB-Schnittstelle des PCs. Nach dem Start stoppt der PC an der Pre-Boot Authentisierung. Es folgt die Abfrage des Token-Passworts.



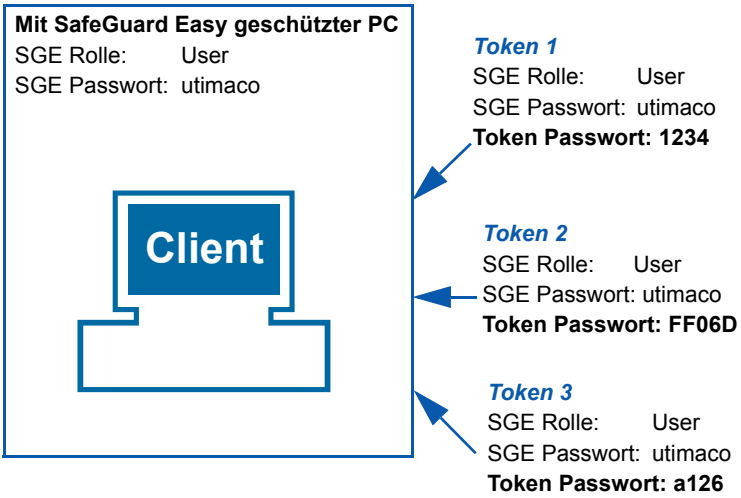
Ist das Token-Passwort korrekt eingegeben, werden die SafeGuard Easy Zugangsdaten vom Token gelesen und anschließend die Anmeldung automatisch durchgeführt.

Verliert ein Benutzer seinen Token, kann der Administrator über Challenge/Response zeitweilig die Anmeldung ohne Token erlauben.

15.1 Vorteile einer Anmeldung mit Token

- Benutzer müssen sich nur das Token-Passwort merken. Die Anmeldung an SafeGuard Easy und das Betriebssystem übernehmen bei entsprechender Konfiguration der Token bzw. der Sichere Automatische Logon (SAL).
- In einem Unternehmen kann ein hierarchisches, zentralisiertes Administrationskonzept eingeführt werden, z.B. für die Erstellung von Konfigurationsdateien.
- In einem Unternehmen bleibt dem „regulären“ Benutzer das SafeGuard Easy-Benutzerkonzept verborgen, weil er seine SafeGuard Easy-Zugangsdaten nicht weiß.
- Kennt der Benutzer die SafeGuard Easy-Zugangsdaten nicht, kann die fehlende Übereinstimmung zwischen SafeGuard Easy und Windows-Benutzer beseitigt und die Zahl der SafeGuard Easy Benutzer pro Arbeitsstation auf eine beliebige Anzahl erhöht werden (Rollenbasierendes Konzept).

  Mit dem **rollen-basierenden Zugriffskonzept** können Sie das SafeGuard Easy Benutzer-Limit von maximal 15 Benutzern pro Arbeitsstation umgehen: Benutzer wissen in einer Rollenumgebung nur ihr Token-Passwort, die SafeGuard Easy-Zugangsdaten kennen sie nicht. Stellt der Administrator etwa eine beliebige Anzahl an USB Token aus, die dieselbe SafeGuard Easy-Zugangsdaten enthalten, können sich beliebig viele Token-Besitzer eine mit SafeGuard Easy geschützte Arbeitsstation teilen. Unterschiedliche Windows-Zugangsdaten garantieren jedem Benutzer seinen individuellen Desktop.


Mit SafeGuard Easy geschützter PC
SGE Rolle: User
SGE Passwort: utimaco
Client
Token 1
SGE Rolle: User
SGE Passwort: utimaco
Token Passwort: 1234
Token 2
SGE Rolle: User
SGE Passwort: utimaco
Token Passwort: FF06D
Token 3
SGE Rolle: User
SGE Passwort: utimaco
Token Passwort: a126

15.2 Unterstützte Token

SafeGuard Easy unterstützt diese Token: Aladdin eToken Pro, Verisign USB Token und RSA SecurID 800-Token.

Aladdin eToken Pro

Aladdin Pro 16K, Aladdin Pro 32K
Aladdin Pro 64K / OTP*

*SafeGuard Easy unterstützt den Kryptochip, aber nicht die Einmal-Passwort-Funktion (OTP=One Time Password) des Tokens.

Aladdin eToken NG-FLASH und NG-OTP

Das Standard-Passwort für (leere) Aladdin eToken ist „1234567890“.

Verisign USB Token

OEM Version des Aladdin eToken.

Die auf den USB Token gedruckte Seriennummer muss mit "ALPR" beginnen.

RSA SecurID 800-Token

SafeGuard Easy unterstützt den Kryptochip, aber nicht die Einmal-Passwort-Funktion (OTP = One Time Password) des Tokens.

ACHTUNG: Sie benötigen eine bestimmte Version des RSA Authenticator Client. Wenden Sie sich für weitere Informationen an Ihren Token-Hersteller. Die RSA Authenticator Utility wird von SafeGuard Easy Version 4.50 nicht mehr unterstützt.

Das Standard-Passwort für RSA SecurID 800-Token ist "PIN_CODE" (Großschreibung beachten!).

15.3 Token-Funktionen

X = wird unterstützt; -- = wird nicht unterstützt

Aktion	Aladdin eToken / VeriSign USB Token	RSA SecurID 800 Token	Lenovo Finger-abdruck-Leser
In der Pre-Boot Authentisierung anmelden	X	X	X
An SafeGuard Easy Administration an-melden	X[1]	X[2]	--
An Konfigurations-dateien anmelden	X[1]	X[2]	--
An Windows anmelden	X[1]	X[2]	X[3]
Windows Arbeitsplatz sperren	X[1]	X[2]	--
Schneller SafeGuard Easy Benutzerwechsel	X[1]	X[2]	--

[1] Nur mit "Aladdin Runtime Environment" (PKCS#11 Modul)

[2] Nur mit "RSA Authenticator Client" (PKCS#11 Modul)

ACHTUNG: Für Aufgaben auf Betriebssystemebene benötigen Sie eine bestimmte Version des RSA Authenticator Client. Wenden Sie sich für weitere Informationen an Ihren Token-Hersteller. Die RSA Authenticator Utility wird von SafeGuard Easy Version 4.50 nicht mehr unterstützt.

[3] Nur mit Lenovo Thinkvantage Fingerprint Software

15.4 Token-Unterstützung installieren

So installieren Sie die Token-Unterstützung:

1. Starten Sie das SafeGuard Easy Setup.
2. Wählen Sie die Installationsoptionen und den Verschlüsselungsmodus.
3. Wählen Sie in den Konfigurationseinstellungen **Allgemein/ Authentisierung/Anmeldeart**. Hier bestimmen Sie, ob sich ein Benutzer mit Tastatur, Token oder Fingerabdruck an der Pre-Boot Authentisierung anmeldet.

Tastatur	Benutzer melden sich mit den SafeGuard Easy- Zugangsdaten in der PBA an.
Aladdin eToken	Benutzer melden sich mit Token-Passwort des Aladdin eTokens in der PBA an.
Fingerprint	Benutzer melden sich mit Fingerabdruck in der PBA an.
RSA SID 800	Benutzer melden sich mit Token-Passwort des RSA SID Token an.
RSA SID 800 Random	Benutzer melden sich mit Token-Passwort des RSA SID Token an. "Random" bedeutet, dass ein Zufallspass-wort auf den Token geschrieben wird. Dieses Zufallspasswort wird in SafeGuard Easy für die Authentisierung registriert. Benutzer kennen dieses Passwort nicht.

4. Wenn Sie einen Token (Aladdin, RSA) oder den Fingerabdruck ausgewählt haben, wählen Sie die **Anmeldemethode.**

Nur mit Token	Alle SafeGuard Easy-Benutzer müssen sich mit einem Token in der Pre-Boot Authentisierung anmelden. ***ACHTUNG:*** Im Modus "Nur mit Token" müssen Sie einen Token mit SafeGuard Easy-Zugangsdaten besitzen. Mit einem „leeren“ Token können Sie sich sonst nach der Installation bei aktivierter Pre-Boot Authentisierung nicht mehr an Ihrem PC anmelden!
Wahlweise mit Token (empfohlene Installationsmethode)	Benutzer melden sich entweder mit Token oder durch manuelle Eingabe der SafeGuard Easy-Zugangsdaten in der Pre-Boot Authentisierung an.

5. Wenn Sie „Wahlweise mit Token“ gewählt haben, bestimmen Sie über **Benutzer/<Benutzername>/ Anmeldeart**, wer sich mit Token anmelden muss.

   Sie können z.B. dem Benutzer User die Anmeldung mit Token vorschreiben (Einstellung "Erforderlich"), Benutzer SYSTEM hat dagegen die Wahl zwischen Token und manueller Eingabe der SafeGuard Easy-Zugangsdaten (Einstellung "Nicht erforderlich").

6. Definieren Sie unter **Allgemein/Anmeldung/Ausstellungsmodus**, wer SafeGuard Easy-Zugangsdaten auf einen Token schreiben darf. Es gibt diese Ausstellungsvarianten:

Benutzer	Benutzer kann in der Pre-Boot Authentisierung immer einen „leeren“ Token ausstellen. „Leer“ bedeutet, dass sich keine SafeGuard Easy-Zugangsdaten auf dem Token befinden.
Externe Bestätigung	Benutzer muss den Helpdesk anrufen und erhält per Challenge Response die Erlaubnis, einen Token in der Pre-Boot Authentisierung auszustellen
Zentral	Benutzer erhält einen ausgestellten Token und darf den Token nie in der Pre-Boot Authentisierung ausstellen.

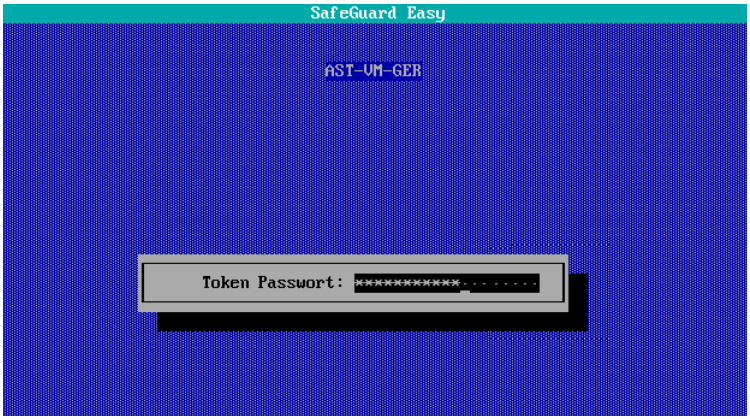
7. Schließen Sie die Installation ab. Sie haben nun alle Einstellungen für eine Token-Anmeldung getroffen.
8. Starten Sie den PC neu.

15.5 Das erste Mal mit Token in der Pre-Boot Authentisierung anmelden

So melden Sie sich mit einem formatierten, „leeren“ Token an:

1. Stecken Sie den Token in den USB Port.
2. Schalten Sie den PC ein und warten Sie, bis der Rechner an der Pre-Boot Authentisierung stoppt.
3. Geben Sie das Token-Passwort ein

   Standard für Aladdin eToken:1234567890.
   Standard für RSA SID 800 Token: PIN_CODE

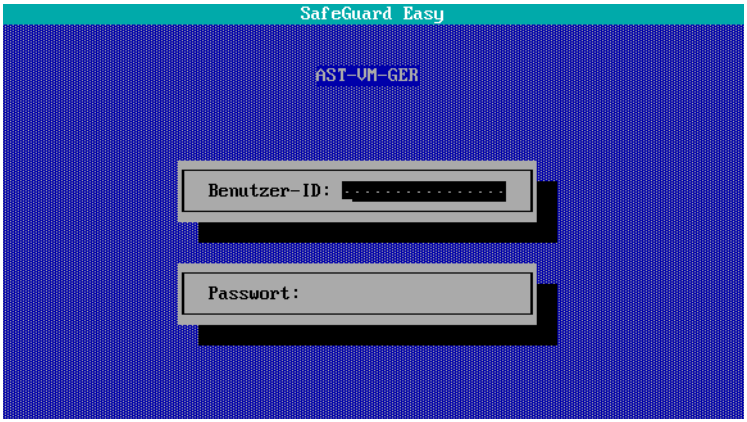


4. Es wird daran erinnert, dass das Standard Passwort des Token ein Sicherheitsrisiko darstellt und geändert werden muss (maximal 32 Zeichen möglich).

   Geben Sie ein neues Token-Passwort ein.

5. Geben Sie die SafeGuard Easy-Zugangsdaten (Benutzername und Passwort) ein. Die Daten werden auf den Token geschrieben

   Der eingestellte Ausstellungsmodus regelt, ob ein Benutzer SafeGuard Easy-Zugangsdaten selbst auf den Token schreiben darf!



6. Die Anmeldung an SafeGuard Easy wird ausgeführt. Bei der nächsten Anmeldung genügt das Token Passwort.

15.6 Token-Passwort ändern

So ändern Sie das Token-Passwort in der Pre-Boot Authentisierung:

1. Stecken Sie den Token in den USB-Port.
2. Starten Sie den PC.
3. Geben Sie das Token-Passwort in der Pre-Boot Authentisierung ein.
4. Drücken Sie die Taste [F10].
5. Geben Sie ein neues Token-Passwort ein.

Für neue Token-Passworte gelten folgende Regeln:

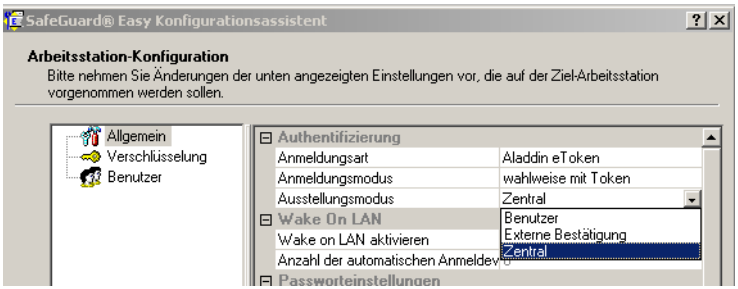
- Das neue Token-Passwort darf nicht gleich dem Alten sein.
- Das neue Token-Passwort darf nicht trivial sein (z.B. „1234“ oder „asdf“).

15.7 SafeGuard Easy-Zugangsdaten auf dem Token ändern/löschen

Die SafeGuard Easy-Zugangsdaten werden über die Token Administration gelöscht oder geändert (siehe auch ’Token mit der Token Administration zentral ausstellen’).

15.8 Token ausstellen

Beim „Ausstellen“ werden Daten auf den Token geschrieben, die dann für die Authentisierung verwendet werden.



Der "Ausstellungsmodus" gibt an, wer SafeGuard Easy-Zugangsdaten auf den Token schreiben darf.

Dem Benutzer, der den Token ausstellt, muss das Token-Passwort bekannt sein. Ansonsten ist es keiner Instanz möglich, den Token auszustellen.

15.8.1 Token-Ausstellungsmodus

Ausstellungsmodus „Benutzer“

Ein Benutzer darf nach erstmaligem Erscheinen der Pre-Boot Authentisierung selbständig seine SafeGuard Easy-Zugangsdaten auf einen leeren Token schreiben. Voraussetzung ist natürlich, dass die Zugangsdaten eines SafeGuard Easy-Benutzerprofils dem Benutzer bekannt und auf der Arbeitsstation vorhanden sind.

Ausstellungsmodus „Externe Bestätigung“

Ein Benutzer darf nur nach dem Austausch von Challenge und Response Code den Token mit SafeGuard Easy-Zugangsdaten ausstellen.

Der Benutzer muss in diesem Fall durch Drücken der Taste [F9] in der Pre-Boot Authentisierung einen Challenge Code anfordern und sich mit dem Administrator in Verbindung setzen. Der Administrator startet den Response Code Assistenten, befüllt die Dialoge zur Authentisierung und gibt den Challenge Code ein. Als „Auszuführende Aktion“ wählt er „Erlaubnis zum Ausstellen eines Tokens erteilen“.

Der erzeugte Response Code wird dann per Mail, SMS oder Telefon an den Benutzer übermittelt. Der Benutzer trägt den Response Code in die dafür vorgesehenen Felder ein. Danach darf er SafeGuard Easy-Zugangsdaten auf den Token schreiben.

Diese Option involviert eine zentrale Stelle in einem Unternehmen (Administrator) und verursacht unter Umständen höheren Zeit- und Arbeitsaufwand. Es wird jedoch im Gegenzug gewährleistet, dass der Administrator immer benachrichtigt wird, wenn für eine Maschine ein Token ausgestellt werden soll.

Ausstellungsmodus „Zentral“
Der Benutzer erhält einen ausgestellten Token von zentraler Stelle und kann sich anmelden. Die zentrale Ausstellung des Token übernimmt die Token Administration. Details zum Ausstellen eines Token mit der Token Administration lesen Sie bitte unter ’Token mit der Token Administration zentral ausstellen’ nach.

15.8.2 Token-Ausstellung automatisieren

Es besteht die Möglichkeit, die Ausstellung von Token zu automatisieren. Hierzu erstellt die Einrichtung, die die Token ausstellt, ein Visual Basic-Script (*.vbs), das in einem Schritt gewünschte Anmeldeinformationen (Windows, Terminal Server, SafeGuard Easy etc.) auf die Token schreibt. Dieses Verfahren eignet sich insbesondere für die Erstausstellung einer großen Anzahl von Token.

Beispielskript

Die folgende Liste zeigt ein Beispielskript. Editierbare Einträge stehen in Klammer und sind kursiv hervorgehoben, z.B. *<PIN des Token>*.

```
dim scard
dim res
dim slotID
dim pin
dim mustChangePIN
dim userID
dim password
dim domain
dim terminalServer
dim fileName
dim cerFile
dim linkFile
dim pkcsFile
dim protFile
dim cardInserted
dim authFile
dim configFile

set scard = WScript.CreateObject(„SCardAdmScriptAPI.SCScriptAPI“)

' *** Initialisieren WICHTIG !!!! ***
slotID = 0
res = scard.Initialize(slotID)

' *** Karte eingelegt ? ***
cardInserted = scard.IsCardInserted()
if cardInserted then
WScript.Echo(„Card is inserted“)
else
WScript.Echo(„NO Card in Slot“)
end if
```

```
' *** Seriennummer auslesen ***
serialNumber = scard.GetCardSerialNumber()
WScript.Echo(serialNumber)

' *** User PIN ändern ***
pin=„<Neue Benutzer-PIN>“
oldPIN=„<Bisherige Benutzer-PIN>“
res = scard.SetUserPIN(oldPIN,pin)

' *** SO PIN ändern ***
pin=„<Neue Security Officer-PIN>“
oldPIN=„<Bisherige Security Officer-PIN>“
res = scard.SetSOPIN(oldPIN,pin)

' *** User PIN Initialisieren ***
pin=„<Neue Benutzer-PIN>“
soPIN=„<Security Officer-PIN des Token>“
res = scard.InitUserPIN(soPIN,pin)

' *** Anmelden ***
pin = „<PIN des Token>“
res = scard.LoginUser(pin)

' *** User PIN Wechsel: 1=Wechsel erzwingen   0=Wechsel nicht erforderlich ***
mustChangePIN = <0, 1>
res = scard.SetUserChangePIN(mustChangePIN)

' *** Windows Account Daten setzen ***
userID = „<Windows-Benutzernamen>“
password = „<Windows-Benutzerpasswort>“
domain = „<Domänennamen>“
res = scard.SetWindowsAccount(userID,password,domain)

' *** SGEasy Account Daten setzen ***
configFile = „<Absoluter Pfad und Name der SafeGuard Easy-Install-Konfigurationsdatei>“
userID = „<SafeGuard Easy-Benutzer, der auf den Token geschrieben wird>“
authFile = „<Absoluter Pfad der Datei, die die Authentisierungsdaten für die
           Konfiguratiosdatei enthält.>
res = scard.SetSGEasyAccount4(configFile,userID,authFile)
WScript.Echo(res)

' *** Windows User ID anzeigen ***
userID = scard.GetWindowsAccount()
WScript.Echo(userID)

' ***MultiDesktop Rolle(n) hinzufügen ***
userID = „<Rollennamen>“
password = „<Passwort zum Rollennamen>“
domain = „<Domänennamen>“
```

```
res = scard.AddMultidesktopRole(userID,password,domain)

' *** Terminal Server Account(s) hinzufügen ***
userID = „<TS-Benutzernamen>“
password = „<TS-Passwort>“
domain = „<Domänennamen>“
terminalServer = „<Name des TS>“
res = scard.AddTerminalServerAccount(userID,password,domain,terminalServer)
```

HINWEISE:

- Löschen Sie die angegebenen Anführungszeichen nicht! Ein Zeileneintrag kann bspw. so aussehen: password=”Vertrieb”. Soll z.B. kein Passwort in ein Feld eingetragen werden, belassen Sie die vorhandenen Anführungszeichen als Platzhalter in der Zeile (z.B. password = ““).
- Geben Sie immer die für den gesteckten Token aktuell gültigen PINs an. Ansonsten bricht das Skript mit einer Fehlermeldung ab.
- Nach Ausführen eines Skripts wird ein schon auf dem Token vorhandener Windows-Account überschrieben.
- Nach Ausführen des Skripts wird auf dem Token eine zusätzliche neue Rolle angelegt. Sind bereits MultiDesktop-Rollen vorhanden, werden diese nicht gelöscht bzw. überschrieben.
- Ist bereits ein Terminal Server Account vorhanden, wird dieser nach Ausführen des Skripts nicht gelöscht bzw. überschrieben.

Erklärung zum Skriptteil "SafeGuard Easy Account Daten setzen"

- **configFile**
  Benennt den absoluten Pfad und Namen der SafeGuard Easy Konfigurationsdatei.

  Beispiel: configFile = “D:\Install.cfg“

  Die Konfigurationsdatei muss vor dem automatisierten Aufbringen mit dem SafeGuard Easy Konfigurationsdateiassistenten erstellt worden sein. Es muss sich hierbei um eine Konfigurationsdatei mit der Eigenschaft „Installieren“ handeln.

  Unbedingt enthalten muss die Konfigurationsdatei diese SafeGuard Easy- Benutzerprofile:

  1) den Benutzer, der unter *userID* auf den Token geschrieben werden soll (z.B. “User“)

  2) den Benutzer, der sich unter *authFile* an der Konfigurationsdatei anmeldet (z.B. “Helpdesk“)

- **userID**
  SafeGuard Easy-Benutzer, der auf den Token geschrieben wird. Dieser Benutzer muss in der Konfigurationsdatei angelegt sein.

  Bsp.: userID = “User“

- **authFile**
  Absoluter Pfad der Datei, die die SafeGuard Easy-Profildaten für die Anmeldung an die Konfigurationsdatei enthält.

  Beispiel.: authFile = “D:\Token.PWD“

  Die verschlüsselte Datei Token.PWD enthält die SafeGuard Easy-Profildaten. Erzeugt wird Token.PWD mit dem Tool SGECP-WF.exe. (liegt auf der SafeGuard Easy-CD im \Tools-Verzeichnis).

Skript ausführen

So führen Sie ein Skript aus:

1. Installieren Sie den Token Support und die Token Administration auf dem Aussteller-PC.
2. Verbinden Sie für Smartcard-Anwendungen einen Smartcard-Leser mit der Arbeitsstation.
3. Schreiben/Kopieren Sie den kompletten aufgeführten Skripttext in einen Editor und speichern Sie die Datei mit der Endung .VBS (z.B. Smartcard.vbs).
4. Passen Sie die editierbaren Felder an.
5. Stecken Sie eine Smartcard in den Kartenleser/einen Token an den Rechner an.
6. Führen Sie das Skript aus (bspw. durch einen Doppelklick im Windows Explorer).
7. Die Smartcard / der Token wird mit den eingetragenen Daten ausgestellt.

15.9 Mit Token an den Administrationswerkzeugen anmelden

SafeGuard Easy besitzt für administrative Aufgaben verschiedene Werkzeuge (Administration, Konfigurationsdateiassistenten, Response Code Assistenten). Bestimmte Aktionen innerhalb dieser Administrationswerkzeuge verlangen SafeGuard Easy-Zugangsdaten, z. B. die Anmeldung an die Administration oder die Authentisierung an einer Basiskonfigurationsdatei im Konfigurationsdateiassistenten.

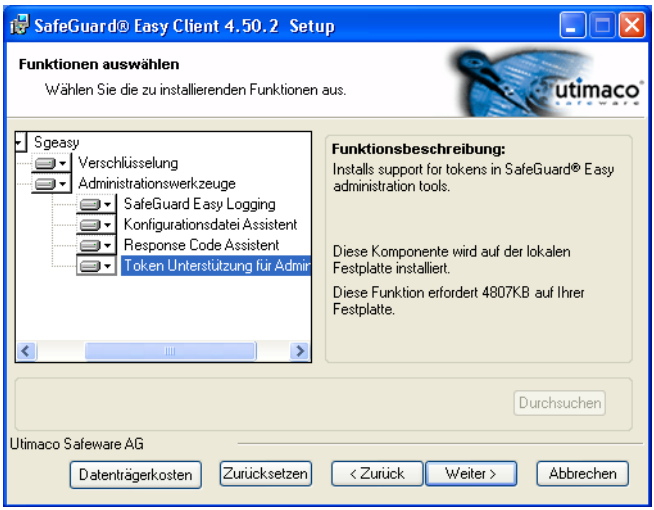
Die Token-Unterstützung in den Administrationswerkzeugen von SafeGuard Easy funktioniert analog zur Anmeldung in der Pre-Boot Authentisierung: Nach Anstecken des Token wird der Benutzer aufgefordert, die PIN anzugeben, das SafeGuard Easy-Passwort und Benutzername werden vom Token gelesen und die Anmeldung bzw. Authentisierung erfolgt.

Die Token-Anmeldung in den Administrationswerkzeugen ist optional und gilt auch für den Fall, dass SafeGuard Easy deinstalliert werden soll.

15.9.1 Token-Unterstützung für die Administrationswerkzeuge installieren

So aktivieren Sie die Token-Unterstützung für die Administrationswerkzeuge:

1. Wählen Sie im SafeGuard Easy-Setup die Option „Token-Unterstützung für Administration“.



2. Starten Sie den PC neu.
3. Installieren Sie folgende Software-Pakete:

Eingesetzter Token	Notwendige Software
Aladdin eToken Verisign USB Token	Aladdin eToken Runtime Environment (siehe auch http://www.utimaco.de/etoken)
RSA SecurID 800	RSA Authenticator Client

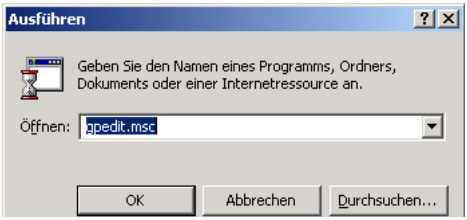
4. Registrieren Sie das #11 Modul des Token.

15.9.2 PKCS#11 Modul des Token registrieren

Um SafeGuard mit dem Token „bekannt" zu machen, müssen Sie das PKCS#11 Modul des Token registrieren.

So registrieren Sie das PKCS#11 Modul:

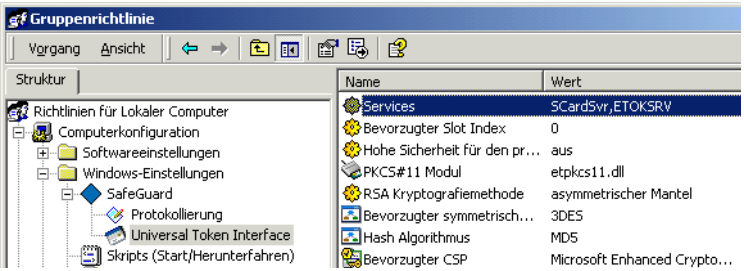
1. Drücken Sie den Windows Start Button und dann *Ausführen*.
2. Geben Sie in den Dialog das Kommando `gpedit.msc` ein.



Die Microsoft Management Konsole (MMC) öffnet sich.

3. Tragen Sie den Service und das PKCS#11-Modul für den Token ein unter
   Computerkonfiguration
   \Windows-Einstellungen
   \SafeGuard\
   \Universal Token Interface

Eingesetzter Token	Notwendige Einstellungen
Aladdin e Token Verisign USB Token	Services: SCardSvr,ETOKSRV PKCS#11 Modul: "etpkcs11.dll" (aus SYSTEM32-Verzeichnis)
RSA SecurID 800	Services: SCardSvr PKCS#11 Modul: "pkcs11.dll" Wenn Sie das PKCS#11-Modul für RSA hinzufügen, achten Sie darauf, den vollen Pfadnamen anzugeben. ACHTUNG: Sie benötigen eine bestimmte Version des RSA Authenticator Client. Wenden Sie sich für weitere Informationen an Ihren Token-Hersteller. Die RSA Authenticator Utility wird von SafeGuard Easy Version 4.50 nicht mehr unterstützt.



4. Speichern Sie die Einstellungen.

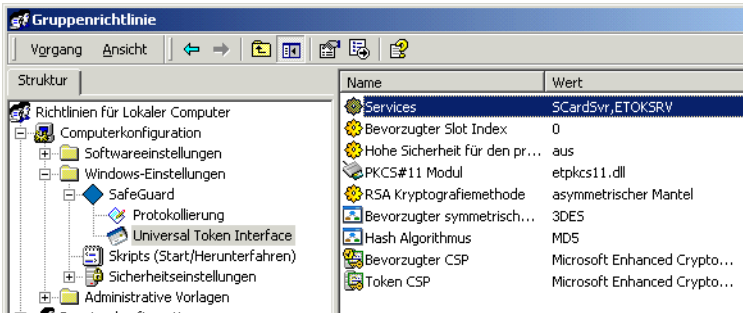
Die Anmeldung an die Administrationswerkzeuge von SafeGuard Easy ist nun mit Token möglich.

15.9.3 Universal Token Interface

Das Universal Token Interface ist ein API, das Utimaco Applikationen verwenden, um mit verschiedenen Token zu kommunizieren. Es stellt einerseits Funktionen zum Zugriff (lesend und schreibend) auf die auf den Token gespeicherten privaten Daten zur Verfügung. Andererseits ermöglicht es die Ver- und Entschlüsselung, das Signieren bzw. die Verifikation von Daten unter Verwendung der auf den Token gespeicherten RSA-Schlüsselpaare.

Das Universal Token Interface wird angezeigt, wenn „Token-Unterstützung für Administration“ installiert ist.
Sie finden die Einstellungen für das Universal Token Interface in der MMC unter:

Computerkonfiguration
\Windows Einstellungen
\SafeGuard
\Universal Token Interface



Folgende Einstellungen können für das Universal Token Interface konfiguriert werden.

Services
Unter Services müssen jene Services angegeben werden, die zum Betrieb des verwendeten Tokens benötigt werden und daher vor der Initialisierung des Universal Token Interfaces gestartet sein müssen.

`SCardSvr`
Betriebssystemeigener Smartcard Service. Dieser Eintrag muss immer vorhanden sein.

Manche Token verlangen darüber hinaus zusätzlich einen token-spezifischen Service, der ebenfalls angegeben werden muss. Die Services müssen durch ein Komma getrennt werden.

Bevorzugter Slot Index
Die Token verlangen bestimmte Slot Indices. Tragen Sie hier den Slot für Ihren Token ein. Wird das PKCS#11 Modul für den SafeGuard Smartcard Provider angegeben, wird der entsprechende Slot 0 automatisch eingetragen.

> ***HINWEIS:***
> Stellen Sie sicher, dass Ihr Token an dem angegebenen Slot angesteckt ist.

PKCS#11 Modul
Das PKCS#11 Modul ist verantwortlich für die Kommunikation (lesen/schreiben) mit dem Token.

Geben Sie hier für Ihren Token das entsprechende PKCS#11 Modul an.

PKCS#11 Module, Services, Slots

Token Provider	Software	PKCS#11 Modul	Services
Aladdin (USB Token)	aktuellstes Aladdin Runtime Environment (RTE)	eTpkcs11.dll	SCardSvr, ETOKSRV
Verisign (USB-Token)	wie Aladdin	wie Aladdin	wie Aladdin
RSA SecurID 800	aktuellster RSA Authenticator Client	pkcs11.dll	SCardSvr

Hohe Sicherheit für den privaten Schlüssel
Wenn Sie diese Option aktivieren, wird der Benutzer bei jeder Operation, die den privaten Schlüssel benutzt, zur Authentisierung (Eingabe der PIN) aufgefordert.

Bevorzugter CSP
Hier werden alle auf dem System verfügbaren CSPs angezeigt. Sie können auswählen, welchen Sie für Operationen mit dem öffentlichen Schlüssel verwenden wollen.

Empfohlen ist die Verwendung des Microsoft Enhanced Cryptographic Service Provider.

Token CSP
Hier müssen Sie den CSP für den von Ihnen verwendeten Token angeben. Wenn Sie Utimaco Smartcards verwenden, müssen Sie den Utimaco Universal Smartcard CSP auswählen.

RSA Kryptografiemechanismus
Für CSPs, die keine direkte RSA Verschlüsselung anbieten, steht der Kryptografiemechanismus die Option **asymmetrischer Mantel** zur Verfügung. Dabei wird das Datenpaket mit einem wählbaren symmetrischen Algorithmus verschlüsselt. Auf den verwendeten Schlüssel wird eine RSA Verschlüsselung angewandt.

Bevorzugter symmetrischer Algorithmus
Wählen Sie hier den Algorithmus für die symmetrische Verschlüsselung des Datenpaketes, wenn Sie **asymmetrischer Mantel** als Kryptographiemethode gewählt haben.

Hash Algorithmus
Wählen Sie hier aus, welcher Hash Algorithmus verwendet werden soll.

15.10 Anmeldung mit Token an das Betriebssystem

Wenn die Anmeldung an SafeGuard Easy erfolgreich war, fordert anschließend das Betriebssystem vom Benutzer gültige Zugangsdaten. Dies bedeutet, dass im Rahmen einer Token-Anmeldung zweimal Benutzerdaten abgefragt werden: Einmal in der Pre-Boot Phase (Token-Passwort) und bei der regulären Anmeldung an das Betriebssystem.

HINWEISE:

- Die SafeGuard-Komponente zur Anmeldung an das Betriebssystem unterstützt maximal 63 Zeichen lange Passworte.

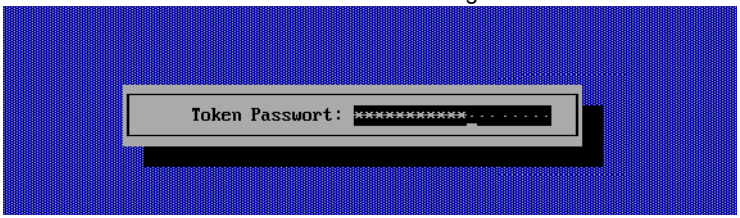
  Utimaco empfiehlt das Maximum beim Token-Passwort nicht zu überschreiten.

- Es wird vorausgesetzt, dass bestimmte Treiber (PKCS#11, Cryptographic Service Provider (CSP)) für die Unterstützung des Tokens auf Betriebssystemebene von den Tokenherstellern zur Verfügung gestellt werden.
  Diese können üblicherweise von den Webseiten der Hersteller heruntergeladen werden und sind dann separat zu installieren.

15.10.1 Betriebssystemdaten auf den Token schreiben

So schreiben Sie Betriebssystemdaten auf den Token:

1. Stecken Sie den (formatierten) Token in den USB Port und starten Sie den PC.
2. Geben Sie an der Pre-Boot Authentisierung das Token-Passwort ein.



3. Das Betriebssystem startet. Geben Sie das Token-Passwort (im Dialog „PIN“ genannt) ein.
4. Der Token enthält noch keine Windows Anmeldedaten. Bestätigen Sie den Dialog Token-Anmeldung mit [Ja].

5. Der Dialog *Token mit Windows-Zugangsdaten ausstellen* wird geöffnet. Geben Sie Ihren Windows Benutzernamen und das Kennwort ein.

Ein Dialog bestätigt die erfolgreiche Ausstellung des Token. Beim nächsten Neustart des PCs werden Sie automatisch an Windows angemeldet.

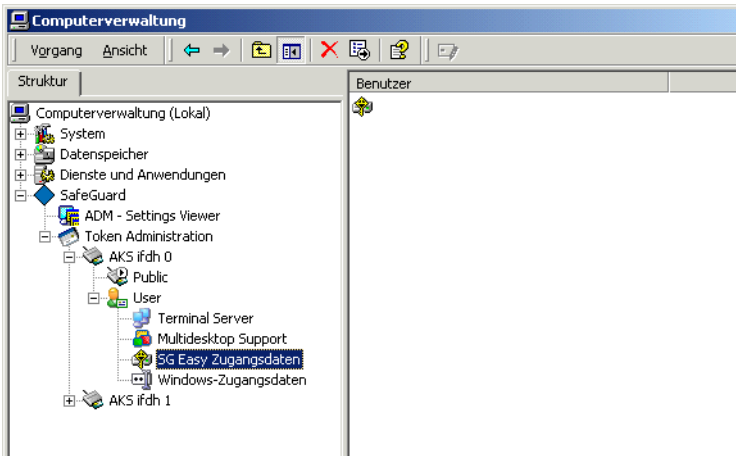
15.10.2 Gespeicherte Windows-Daten in der SAL-Datei

Die Betriebssystem-Daten werden nach jeder erfolgreichen Anmeldung mit Token mit der verschlüsselten SAL-Datei `SGSAL.dat` (zu finden unter <Systemlaufwerk>`/System32`) synchronisiert, vorausgesetzt **das SafeGuard Easy-Anmeldeverfahren „Wahlweise mit Token“** wurde gewählt. Dies garantiert insbesondere in Notfällen (Benutzer verliert Token mit Windows-Daten o.ä.), dass der Benutzer auf die Daten zurückgreifen kann. Ändert der Benutzer seine Windows-Daten, wird auch die `SGSAL.dat` aktualisiert.

15.11 Token mit der Token Administration zentral ausstellen

Die Token Administration bietet Ihnen eine umfangreiche Hilfestellung beim Vorbereiten und Ausstellen der Token. Ist die Token Administration installiert, können Sie folgende Daten auf der Karte speichern:

- Token-Passwort (PIN)
- SafeGuard Easy-Zugangsdaten
- Windows-Zugangsdaten



MultiDesktop Unterstützung und Terminal Server funktionieren nur in Verbindung mit SafeGuard Advanced Security.

15.11.1 Token Administration installieren

So installieren Sie die Token Administration:

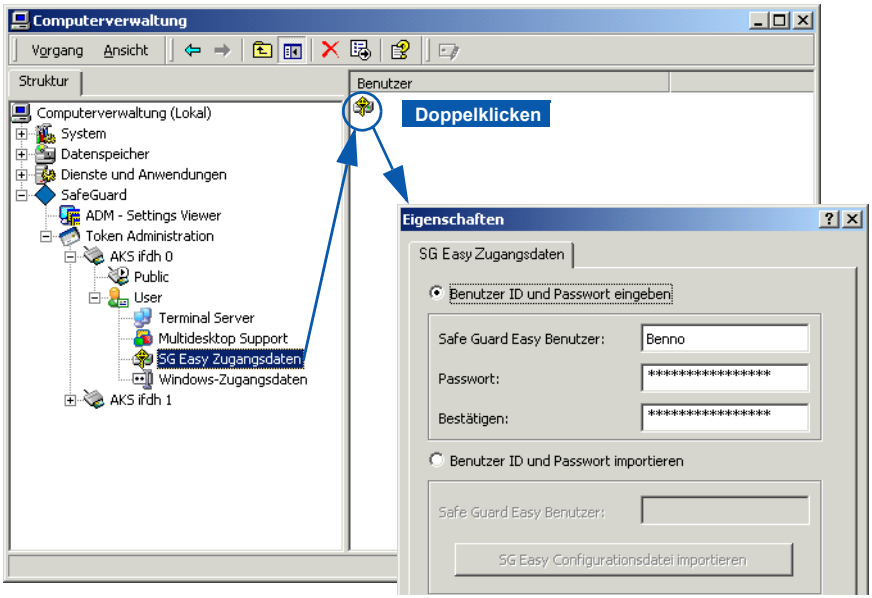
1. Installieren Sie aus dem \TOOLS-Verzeichnis der SafeGuard Easy-CD nacheinander

   - `TokenAdmin.msi`
   - `SCAdmin_SGEasy.msi`

2. Registrieren Sie nach dem Neustart des PCs das PKCS#11-Modul des Token (Details lesen Sie unter 'PKCS#11 Modul des Token registrieren' nach).
3. Verbinden Sie den Token mit dem PC.
4. Rufen Sie die **Computerverwaltung** über Start / Einstellungen / Systemsteuerung / Verwaltung auf.

   Im Ordner „SafeGuard“ der Computerverwaltung erscheint die „Token Administration“.

5. Melden Sie sich an die Token Administration mit Ihrem Token-Passwort an.
6. Öffnen Sie den Ordner **Benutzer**.
7. Markieren Sie den Ordner **SGEasy Zugangsdaten**.
8. Öffnen Sie den Dialog **Eigenschaften** durch einen Doppelklick auf das SafeGuard Easy-Symbol in der „Benutzer”-Spalte
9. Markieren Sie „Benutzer-ID und Passwort eingeben” und tragen Sie Benutzername und Passwort ein.



10. Bestätigen Sie Ihre Eingaben mit [OK].

Auf dem Token sind nun Ihre SafeGuard Easy-Zugangsdaten gespeichert.

Weitere Informationen zu diesem Thema erhalten Sie in der Utimaco-Wissensdatenbank http://www.utimaco.de/myutimaco.

Nutzen Sie bitte die Suchfunktion der Wissensdatenbank, um nach Stichworten wie „Token Admin“ zu suchen.

15.11.2 SafeGuard Easy-Zugangsdaten auf dem Token löschen

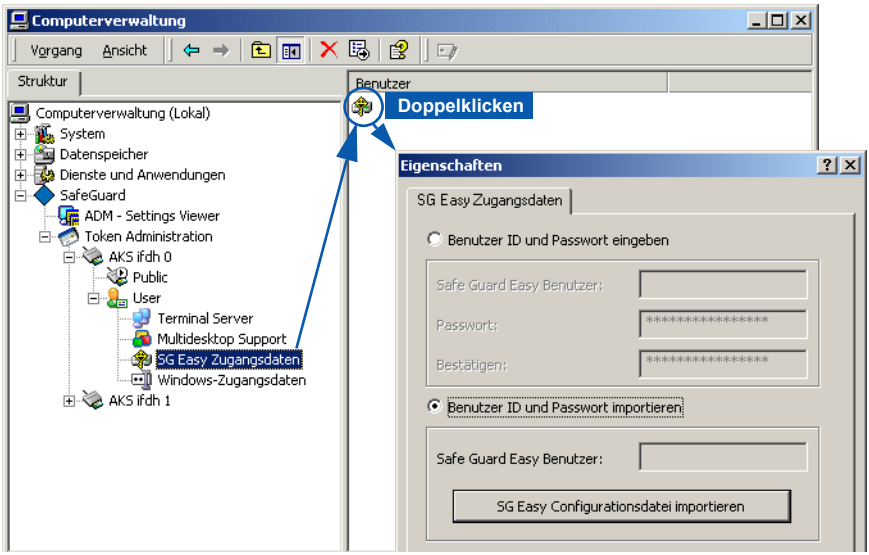
Entfernt werden Token-Daten über den Befehl „Löschen“ im Kontextmenü von „SGEasy Zugangsdaten“.

15.11.3 SafeGuard Easy-Zugangsdaten aus Konfigurationsdatei importieren

Bei einem Import werden die SafeGuard Easy-Benutzerdaten (Name und Passwort) aus einer bestehenden Konfigurationsdatei auf den Token geschrieben. Diese Vorgehensweise bietet sich an, wenn dem Aussteller das SafeGuard Easy Benutzerpasswort nicht bekannt ist bzw. nicht bekannt sein soll.

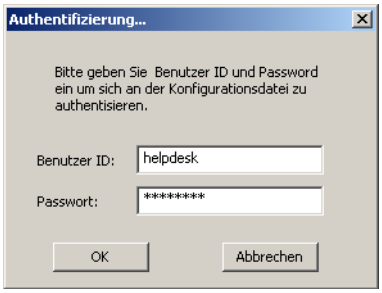
So importieren Sie SafeGuard Easy-Zugangsdaten aus einer Konfigurationsdatei:

1. Starten Sie die Token Administration.
2. Öffnen Sie den Ordner "User".
3. Markieren Sie den Ordner „SG Easy Zugangsdaten“.
4. Doppelklicken Sie auf das Schlüsselsymbol.

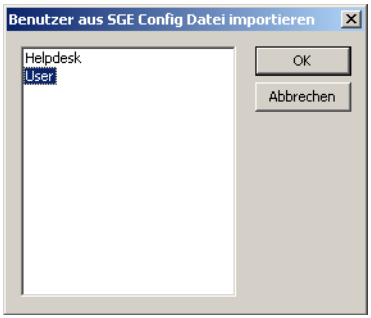


5. Wählen Sie die Option „BenutzerID und Passwort importieren“.

6. Drücken Sie die Schaltfläche [SG Easy Konfigurationsdatei importieren] und wählen Sie eine Konfigurationsdatei aus.
7. Melden Sie sich an die Konfigurationsdatei mit einem SafeGuard Easy-Benutzerprofil an, das in der Konfigurationsdatei angelegt ist.



8. Wählen Sie aus der angezeigten Liste einen Benutzer aus.



9. Drücken Sie [OK], die Daten werden auf den Token geschrieben.

15.12 SafeGuard Easy-Benutzer schnell wechseln

In der Regel besitzen SafeGuard Easy-Benutzer, die gemeinsam einen PC nutzen, die gleichen Rechte. Manchmal kommt es jedoch vor, dass sich Benutzer mit unterschiedlichen SafeGuard Easy-Rechteprofilen einen PC teilen. Im Normalfall (ohne Token-Anmeldung) ist ein SafeGuard Easy-Benutzerwechsel dann nur möglich, wenn der PC komplett heruntergefahren wird und sich der neue Benutzer in der Pre-Boot Authentisierung mit seinen Profildaten anmeldet. Dies kann unter Umständen viel Zeit in Anspruch nehmen. Benutzer begrüßen es jedoch, wenn zwischen Abmeldung des alten Benutzers und Erscheinen des Desktops des neuen Benutzers möglichst wenig Zeit vergeht.

Zeitaufwendiges Neustarten des PCs für einen SafeGuard Easy-Benutzerwechsel ist nicht notwendig, wenn Token eingesetzt werden. In diesem Fall genügt eine einfache Windows-Abmeldung **des „alten“ Benutzers**. Im Windows-Anmeldedialog steckt der **„neue“ Benutzer** dann seinen Token in den USB-Port, authentisiert sich mit der PIN und wird mit dem auf dem Token gespeicherten SafeGuard Easy- (und Windows)-Rechteprofil angemeldet.
Voraussetzung für den Benutzerwechsel ist jedoch, dass die Pre-Boot Authentisierung aktiviert ist und wenigstens einmal gültige SafeGuard Easy-Zugangsdaten dort eingetragen wurden.

15.12.1 Voraussetzungen

1. Installieren Sie SafeGuard Easy und aktivieren Sie die Pre-Boot Authentisierung.
2. Schreiben Sie SafeGuard Easy- und Windows-Daten auf den Token.
3. Beenden Sie die Windows-Sitzung über Start / Beenden / „<Benutzer> abmelden“ oder [Strg]+[Alt]+[Entf]+[Abmelden] beenden.

15.12.2 Beispiel

So funktioniert der schnelle SafeGuard Easy-Benutzerwechsel.

1. Benutzer 1 steckt seinen Token, schaltet den PC ein.
2. Die Pre-Boot Authentisierung erscheint. Benutzer 1 gibt das Token-Passwort in der Pre-Boot Authentisierung an.

   Auf dem Token befinden sich diese SafeGuard Easy-Profildaten:
   Benutzername: Benutzer1
   Passwort: Passwort1
   SafeGuard Easy-Rechte: Keine

   Sind auch Windows-Daten auf dem Token gespeichert, wird der Benutzer ohne weitere Angaben automatisch an SafeGuard Easy und Windows angemeldet.

   Das SafeGuard Easy-Profil von Benutzer 1 ist aktiv. Der Benutzer hat keine SafeGuard Easy-Rechte.
3. Benutzer 1 beendet seine Arbeit, meldet sich von Windows über START / BEENDEN / „Benutzer 1 abmelden“ ab (Alternativ: [Strg]+[Alt]+[Entf]+[Abmelden]).
4. Benutzer 1 zieht nach dem Abmelden seinen Token.

5. Der Windows-Anmeldedialog erscheint.
6. Benutzer 2 steckt seinen Token mit SafeGuard Easy und Windows-Daten in den USB-Port, gibt sein Token-Passwort ein und wird mit diesen SafeGuard Easy-Profildaten angemeldet.

   Benutzername: Benutzer2
   Passwort: Passwort2
   SafeGuard Easy-Rechte:Diskettenverschlüsselung schalten

   Das SafeGuard Easy-Profil von Benutzer 2 ist aktiv. Der Benutzer darf die Diskettenverschlüsselung ein-/ausschalten.

15.13 Hilfe im Notfall

Für folgende Szenarien kann die Notfallhilfe notwendig sein:

- Benutzer verliert Token
- Benutzer vergisst Token z. B. zu Hause
- Benutzer weiß das Token-Passwort nicht mehr

In allen Fällen hilft das Challenge/Response-Verfahren von SafeGuard Easy. Das Challenge-Response-Verfahren unterstützt den Administrator, indem es u.a. eine bestimmte Anzahl an Anmeldungen ermöglicht, ohne dass der Benutzer seinen Token benötigt.

Der Einsatz von Challenge-Response dient also dazu, dem Benutzer den Zutritt zum System zu ermöglichen, wenn der Token nicht verfügbar ist oder das Token Passwort vergessen wurde. Durch das Verfahren wird dennoch sichergestellt, dass sich nur ein legitimer Benutzer anmelden kann.

15.13.1 Voraussetzungen

Für eine erfolgreiche Hilfe im Notfall muss SafeGuard Easy auf dem Safe Guard Easy Client mit folgenden Token-Einstellungen installiert sein:

- Anmeldemodus: Wahlweise mit Token
  (siehe Allgemein/Authentifizierung/Anmeldemodus)
- Anmeldungsart: Erforderlich
  (siehe Benutzer/<Benutzername>/Anmeldung)

HINWEISE:

- Der Benutzer muss die Daten des SafeGuard Easy-Benutzers auf seinem PC wissen! Ansonsten ist es nicht möglich, das Challenge/Response-Verfahren einzuleiten (außer der Administrator teilt dem Benutzer die Daten eines weiteren SafeGuard Easy Benutzers mit).
- Ein permanentes Deaktivieren der Token-Unterstützung ist über Challenge/Response nicht möglich.

15.13.2 Einsatzbeispiele

Im folgenden soll beispielhaft dargestellt werden, welche Aufgaben Benutzer und Administrator zukommen, wenn ein Benutzer den Token vergisst/verliert oder das Token-Passwort nicht mehr weiß.

Für alle Beispiele müssen folgende Vorgaben am SafeGuard Easy Client erfüllt sein:

- Anmeldungsmodus: Wahlweise mit Token
  (siehe Allgemein/Authentifizierung/Anmeldungsmodus)
- Anmeldungsart: Erforderlich
  (siehe Benutzer/<Benutzername>/Anmeldung)
- Ausstellungsmodus: Benutzer
  (siehe Allgemein/Authentifizierung/Ausstellungsmodus)
- Pre-Boot Authentisierung aktiviert
- Sicherer Automatischer Logon (SAL) aktiviert

Benutzer vergisst Token

Benutzer	Administrator/Support/Helpdesk
Gibt seine SafeGuard Easy-Zugangsdaten in der Pre-Boot Authentisierung ein und fordert mit [F9] den Challenge Code an. Ruft Administrator/Support/Helpdesk an.	
	Versichert sich, dass der Anrufer der tatsächliche Benutzer ist. Startet den Response Code Assistenten. Erfragt den Challenge Code vom Benutzer und trägt ihn ein. Wählt im Response Code im Dialog „Auszuführende Aktion“ die Option „**Anmeldung ohne Token für X Anmeldungen**“. Gibt den erzeugten Response Code an den Benutzer weiter.
Trägt den Response Code in die dafür vorgesehenen Felder ein und darf sich nun X-mal ohne Token an der Pre-Boot Authentisierung anmelden. Für die Anmeldung an das Betriebssystem (Benutzer kennt die Daten nicht) wird in diesem Fall die SAL-Datei geöffnet, die Betriebssystemdaten des Benutzers ausgelesen und die Anmeldung automatisch durchgeführt.	

Benutzer verliert Token

Benutzer	Administrator/Support/Helpdesk
	Sendet dem Benutzer einen (leeren) neuen Token mit Standard-Passwort.
Gibt seine SafeGuard Easy-Zugangsdaten in der Pre-Boot Authentisierung ein und fordert mit [F9] den Challenge Code an. Ruft Administrator/Support/Helpdesk an.	
	Startet den Response Code Assistenten. Erfragt den Challenge Code. Wählt im Response Code im Dialog „Auszuführende Aktion“ die Option „**Erlaubnis zum Ausstellen eines Tokens erteilen**“. Gibt den erzeugten Response Code an den Benutzer weiter.
Trägt den Response Code in die dafür vorgesehenen Felder ein und meldet sich an. Steckt beim nächsten Start des PC den neuen Token an, gibt das Passwort ein und schreibt die SafeGuard Easy-Zugangsdaten auf den Token (wenn Token noch nicht ausgestellt). Die Betriebssystemdaten muss der Benutzer nicht selbständig auf den Token schreiben, sie werden bei der Anmeldung automatisch aus der SAL-Datei gelesen und auf den Token gespeichert. Voraussetzung: SafeGuard Easy Token-Anmeldeverfahren ist „Wahlweise mit Token“.	

HINWEIS:
Wenn der Token bereits über die Token Administration ausgestellt wurde, ist kein Challenge/Response-Verfahren nötig.

Benutzer vergisst Token-Passwort

Benutzer	Administrator/Support/Helpdesk
Administrator erlaubt dem Benutzer zunächst über Challenge/Response-Verfahren eine einmalige Anmeldung ohne Token (siehe „Benutzer vergisst Token“)	
Ist über Challenge/Response ohne Token an SafeGuard Easy und Windows angemeldet. Steckt den Token in den USB Port.	
	Verbindet sich über Remote-Funktion (siehe 'Token remote verwalten') der Token Administration auf den PC des Benutzers und ändert das Token-Passwort. Teilt dem Benutzer das neue Token Passwort mit. Voraussetzung für Remote Funktion: - Administrator weiß das Administrator-Passwort des Token. - Benutzer-PC muss im Netzwerk sein - Token Administration muss auf Administrator-PC und Benutzer-PC installiert sein - Token verfügt über ein Administrator-Passwort (= Security Officer PIN).
Startet den PC neu und meldet sich mit dem Token an.	

15.13.3 Token remote verwalten

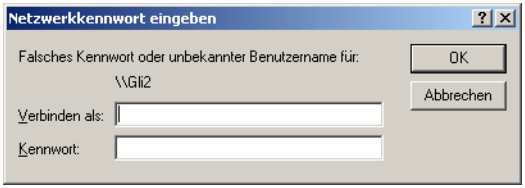
Die Remoteverwaltung dient dazu, Benutzern in Notfallsituationen zu helfen, z.B. wenn sie ihr Token-Passwort vergessen haben und sich nicht mehr anmelden können.

Wollen Sie einen Token remote administrieren, muss

- zwischen Benutzer-PC und Administrator-PC eine Netzwerkverbindung bestehen.
- auf dem Administrator-PC die Token Administration vorhanden sein.
- auf dem Benutzer-PC die Token-Unterstützung und die Token Administration installiert und der Token an die Arbeitsstation angeschlossen sein.
- der Administrator die Security Officer PIN des Benutzer-Tokens kennen.

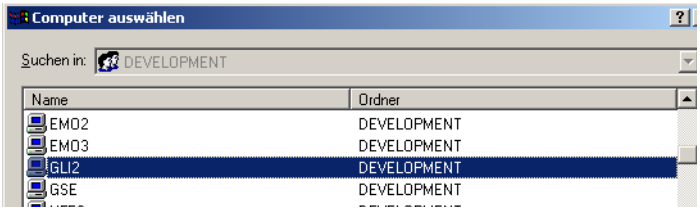
So verwalten Sie Token remote:

1. Authentisieren Sie (Administrator) sich am Benutzer-PC, an dem der Token angeschlossen ist.

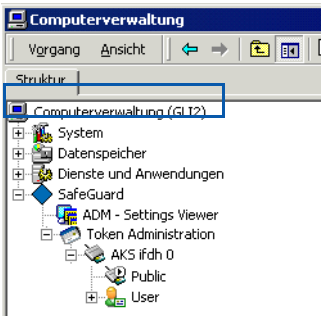


2. Stellen Sie über die Computerverwaltung erneut eine Verbindung zum Benutzer-PC her.

3. Wählen Sie den Benutzer-PC aus.



4. Öffnen Sie die Token Administration über die Computerverwaltung des Administrator-PCs.



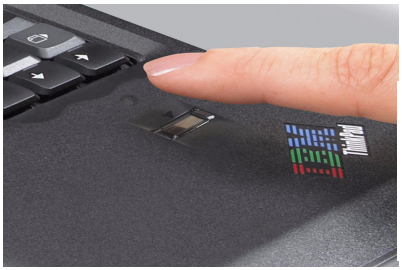
5. Melden Sie sich mit dem Administrator-Passwort (= Security Officer PIN) an den Token des Benutzers an.

Sie können nun eine neue Benutzer-PIN vergeben, Token deblockieren etc.

16 Mit Lenovo Fingerabdruck-Leser anmelden

Benutzer müssen sich heutzutage unterschiedliche Ziffernkombinationen merken, um Zugang zu ihrem Notebook/PC zu erhalten. Im Unterschied zu einem Token oder Passwort ist ein Fingerabdruck einmalig und kann nicht erraten (Passwort) oder vergessen (Token) werden.

Fingerabdruck-Leser sind direkt in bestimmte Lenovo Notebooks integriert. Die Anmeldung per Fingerabdruck ist aber auch möglich über externe USB-Tastaturen oder USB-Leser.



SafeGuard Easy verknüpft einen Finger des Benutzers mit SafeGuard Easy-Zugangsdaten. Es genügt für eine Anmeldung also, den Finger über den Leser zu führen, die Anmeldung an SafeGuard Easy erfolgt automatisch.

Vorteile einer Anmeldung mit Fingerabdruck

- Sicherheit: Kein Passwort oder Token zur Anmeldung nötig
- Komfort: Automatische Anmeldung an SafeGuard Easy und Windows (bzw. alle Anwendungen, die eine Authentisierung verlangen)

HINWEIS:
Es wird nur ein einziger angeschlossener Fingerabdruck-Leser akzeptiert.

X = wird unterstützt; -- = wird nicht unterstützt

Aktion	Lenovo Fingerabdruck-Leser
In der Pre-Boot Authentisierung anmelden	X[3]
An SafeGuard Easy Administration anmelden	--
An Konfigurationsdateien anmelden	--
An Windows anmelden	X[3]
Windows Arbeitsplatz sperren	--
Schneller SafeGuard Easy Benutzerwechsel	--

[3] Nur mit Lenovo Thinkvantage Fingerprint Software

16.1 Voraussetzungen

- Lenovo-PC / Lenovo-Notebook der Serien 5x oder 6x
- aktuelles BIOS wird empfohlen
- Lenovo Fingerprint Leser in Notebook, USB Tastatur mit Fingerprint Reader, USB Fingerprint Reader
- SafeGuard Easy ab Version 4.30
- unterstützte Thinkvantage Fingerprint-Software (Minimum):
  - Thinkvantage Fingerprint Software 5.5.0
  - Thinkvantage Fingerprint Software 5.60/5.61
    Ab Version 5.60/5.61 muss im Registry-Zweig
    HKEY_LOCAL_MACHINE
    SOFTWARE
    Protector Suite QL
    1.0

    der DWORD-Wert "**BiosFeatures**" auf "2" gesetzt werden.

16.2 Unterstützte Hardware

SafeGuard Easy unterstützt zur Authentisierung mit dem Fingerabdruck Lenovo PC-/Notebook-Serien, die seit Herbst 2005 auf dem Markt sind.

Unterstützte Notebook-Serien	Z60/Z61
	T60/T61
	X60/X61
	R60

Unterstützte Desktop-Serien	A51
	A52
	M51
	M52
	M52e

Nicht unterstütze Notebook-Serien	3000
	T4x

Nicht unterstütztes Tablet PC Notebook	X41
	R61

HINWEISE:

Die Lenovo 3000 Notebook-Serie wird nicht unterstützt, da sie einen Fingerabdruck-Leser von einem anderen Anbieter nutzt.

Tablet PCs benötigen für Anmeldung mit Fingerabdruck eine angeschlossene Tastatur. Eine Eingabe per Tastatur wird in der Pre-Boot Authentisierung benötigt, um die SafeGuard Easy-Zugangsdaten mit dem Fingerabdruck zu verbinden! Handschriftliche Erkennung ist bei der Pre-Boot Authentisierung nicht möglich.

16.3 Unterstützung für Lenovo Fingerabdruck installieren

> ***ACHTUNG:***
> Bei der Anmeldung mit Fingerabdruck wird die SafeGuard Easy-Funktion "Standardbenutzer" nicht unterstützt. Ein SafeGuard Easy-Benutzer, der mit einem Fingerabdruck verknüpft werden soll, muss immer Benutzernamen und Passwort von SafeGuard Easy kennen.

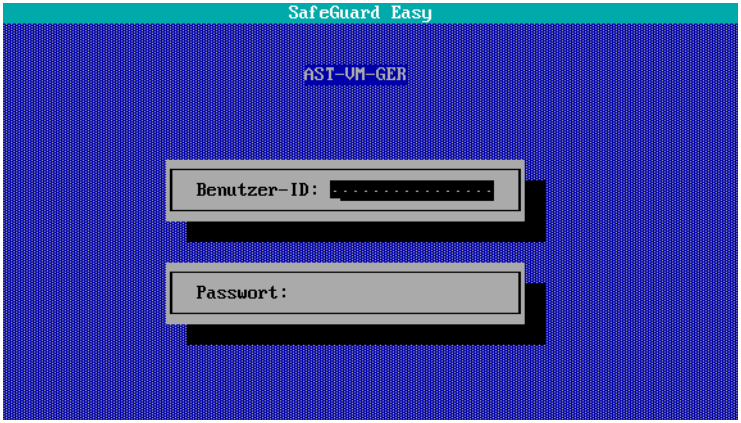
So installieren Sie die Fingerabdruck-Unterstützung:

1. Installieren Sie die Thinkvantage Fingerprint Software (wenn nicht schon vorhanden).
2. Enrollen Sie einen oder mehrere Finger mit der Fingerprint Software. Das Enrollen verknüpft die Finger mit den Windows-Anmeldedaten. Wie man einen Finger enrollt, finden Sie in der Hilfe zur Thinkvantage Fingerprint Software oder unter http://www-307.ibm.com/pc/support/site.wss/document.do?lndocid=MIGR-58403.
3. Um den Fingerabdruck zu testen, starten Sie den PC/das Notebook neu. Führen Sie nach dem Neustart einen der enrollten Finger über den Leser. Sie werden automatisch an Windows angemeldet

4. Starten Sie das Control Center der Thinkvantage Fingerprint Software.
5. Beim ersten Enrollen eines Fingers wird nachgefragt, ob dieser auch für "Power-On" verwendet werden soll. Klicken Sie auf [JA].
6. Installieren Sie SafeGuard Easy.

7. Markieren Sie in den Konfigurationseinstellungen unter **Allgemein / Authentisierung / Anmeldeart** die Option "Fingerabdruck".
8. Starten Sie den PC neu.
9. Führen Sie nach den Neustart einen der enrollten Finger über den Leser.

10. Die Pre-Boot Authentisierung erscheint. Es werden jedoch keine Daten abgefragt, nur die Zeile "Starte Authentifizierung per Fingerabdruck-Leser (weiter mit bel. Taste)" wird angezeigt.
11. Die Fingerprint-Anmeldung erscheint. Führen Sie nun den Finger über den Leser, der mit SafeGuard Easy-Daten verknüpft werden soll. Der Finger muss bereits über die Thinkvantage Fingerprint Software enrollt worden sein!
12. Die Pre-Boot Authentisierung erscheint. Geben Sie nun die SafeGuard Easy-Zugangsdaten ein, die zur Authentisierung mit Fingerabdruck verwendet werden.



13. Verknüpfen Sie über die Taste [F6] einen weiteren Finger mit den SafeGuard Easy-Zugangsdaten für den Fall, dass der Erste nicht erkannt wird, z. B. wegen einer Verletzung.
14. Die Verknüpfung mit den Fingern ist nun hergestellt. Bei jedem Neustart des PCs/Notebooks genügt nun das Präsentieren eines enrollten Fingers zur Anmeldung an SafeGuard Easy und Windows.

HINWEISE:

Benutzer brechen mit der Taste [Esc] die Fingerabdruck-Anmeldung ab und melden sich mit SafeGuard Easy-Benutzernamen und Passwort an.

Der Abbruch über [Esc] ist notwendig, wenn

- die Fingerabdruck-Authentisierung installiert wird, an den PC/das Notebook aber kein Fingerabdruckleser angeschlossen ist
- sich der Benutzer nicht mit Fingerabdruck anmelden kann oder der Fingerabdruck-Leser defekt ist. Über die Taste [Esc] geht er zurück in die Pre-Boot Authentisierung. Dort kann er sich wie gewohnt mit SafeGuard Easy-Benutzernamen und Passwort (nur Passwort für Standardbenutzer) anmelden.

16.4 SafeGuard Easy-Passwort ändern

Benutzer ändern ihr Passwort

- in der Pre-Boot Authentisierung.
- in der SafeGuard Easy-Administration.

So ändern Sie das Passwort in der Pre-Boot Authentisierung:

1. Starten Sie den PC. Die Fingerprint-Anmeldung erscheint.
2. Drücken Sie [Esc]. Die Pre-Boot Authentisierung erscheint.
3. Geben Sie Ihre SafeGuard Easy-Zugangsdaten ein.
4. Drücken Sie [F10] und ändern Sie das Passwort.
   Der PC startet, ohne den Fingerabdruck zu verlangen.
5. Starten Sie den PC erneut. Die Fingerprint-Anmeldung erscheint.
6. Führen Sie den Finger über den Leser. Die Pre-Boot Authentisierung erscheint.
7. Geben Sie Ihren Benutzernamen und das neue Passwort ein (Standardbenutzer nur das Passwort).
8. Bestätigen Sie mit der Eingabe-Taste. Die Fingerabdruck-Anmeldung erscheint.
9. Führen Sie den Finger über den Leser. Die SafeGuard Easy-Daten werden mit dem Finger verknüpft und die Anmeldung ausgeführt.

Das Passwort wurde neu gesetzt.

So ändern Sie das Passwort in der SafeGuard Easy-Administration:

1. Starten Sie die Administration über Programme/Utimaco/SafeGuard Easy/Administration.
2. Wählen Sie den Ordner "Benutzer" und ändern Sie Ihr Passwort unter "Passwort konfigurieren".
3. Starten Sie den PC neu. Die Fingerprint-Anmeldung erscheint.
4. Führen Sie den Finger über den Leser. Die Pre-Boot Authentisierung erscheint mit der Meldung, dass die Daten nicht übereinstimmen.
5. Geben Sie Ihre SafeGuard Easy-Zugangsdaten ein (neues Passwort!). Sie werden angemeldet.

Die neuen SafeGuard Easy-Zugangsdaten und der Fingerabdruck sind nun verknüpft.

16.5 Häufig gestellte Fragen

Benötigt man zusätzliche Software wie Lenovos Client Security Solution (CSS)?

Die SafeGuard Easy-Fingerabdruck-Lösung ist unabhängig von CSS. Sie benötigen nur die Thinkvantage Fingerprint Software zum Enrollen von Fingern.

Werden mehrere Benutzer unterstützt?

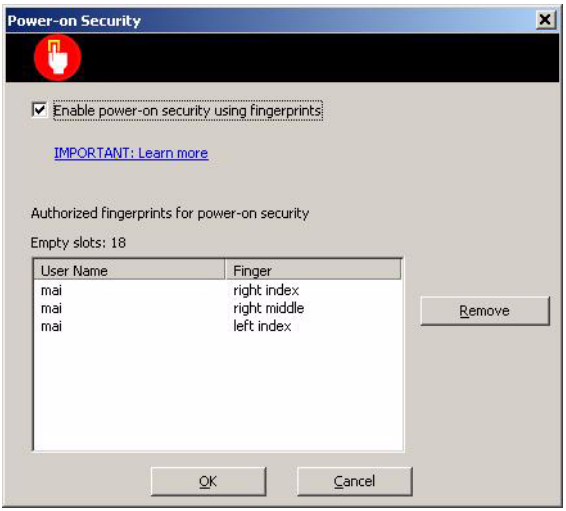
Es gibt auf jedem Leser Platz für 21 Fingerabdrücke. Jedem dieser Fingerabdrücke kann ein beliebiger Windows-Benutzer über die Thinkvantage Fingerprint Software zugeteilt werden. Genauso verhält es sich mit SafeGuard Easy, nur dass die Verknüpfung von Finger und SafeGuard Easy-Benutzerdaten in der Pre-Boot Authentisierung stattfindet (Beispiel: Mehrere Finger für einen SafeGuard Easy-Benutzer ausstellen).

Was passiert, wenn die Fingerabdruck-Anmeldung nicht funktioniert (Gerät defekt o.ä.)?

Über die Taste [Esc] gelangen Benutzer in die Pre-Boot Authentisierung und können sich mit SafeGuard Easy-Benutzername und -Passwort anmelden. Wenn dem Benutzer das Passwort nicht bekannt ist, kann über Challenge/Response ein neues vergeben werden.

Wie löscht man einen Benutzer?

1. Wählen Sie Programme > Thinkvantage > Thinkvantage Fingerprint Software (TFS).
2. Im TFS-Startbildschirm wählen Sie nacheinander Settings > Power On Security. Es erscheint der Dialog "Power-on Security".
3. Markieren Sie einen Benutzer und drücken Sie anschießend Löschen.



17 Windows-Anmeldung konfigurieren

SafeGuard Easy verlangt mit seiner Pre-Boot Authentisierung als erste Systemkomponente eine Authentisierung. Erst nachdem das System mit gültigen SafeGuard Easy-Zugangsdaten aufgesperrt wurde, erscheint der reguläre Windows-Anmeldedialog.

Benutzer finden es aber oft lästig, sich verschiedene Passworte zu merken, um Zugang zu ihrem PC zu erhalten. Dies führt dazu, dass die verschiedenen Passworte bspw. schriftlich notiert werden, was die Sicherheit im Unternehmen stark gefährdet. Vergessene Passworte sorgen in großen Netzwerken außerdem für zusätzlichen Aufwand beim Helpdesk.

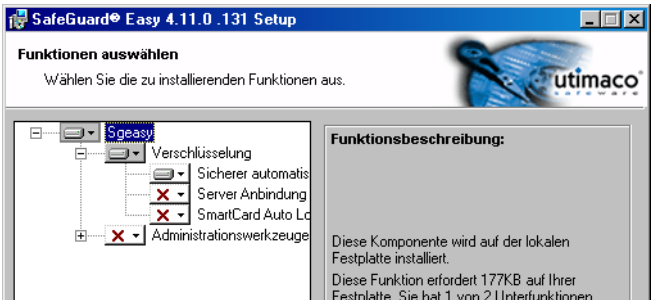
SafeGuard Easy stellt deswegen mit dem Sicheren Automatischen Logon und der Passwortsynchronisierung Funktionalitäten bereit, die den Benutzer von Mehrfachauthentisierungen entlasten und ihn nur noch ein einziges Mal auffordern (nämlich an der Pre-Boot Authentisierung), Benutzerdaten einzutragen.

Um die Windows-Anmeldung noch benutzerfreundlicher zu machen und das Erscheinungsbild des Windows-Anmeldedialog anzupassen, gibt es zusätzliche Optionen in der administrativen Vorlage.

17.1 Sicherer automatischer Logon (SAL)

Die automatische Anmeldung ist eine Komfort-Einrichtung für die Anmeldeprozedur. Ein Benutzer gibt nur einmal seine Windows-Daten ein, bei weiteren Anmeldungen erfolgt die Windows-Anmeldung automatisch und der Benutzer authentisiert sich nur noch mit SafeGuard Easy-Benutzerdaten an der Pre-Boot Authentisierung. SafeGuard Easy nennt dieses Anmeldeverfahren **Sicheren Automatischen Logon** oder kurz **SAL**.

Der SAL kann mit oder ohne Smartcard durchgeführt werden. Dies ist wählbar während der Installation von SafeGuard Easy.



Die automatische Anmeldung an das Betriebssystem ist optional und kann nachträglich mit dem SafeGuard Easy Kommando `Chgsal.exe` ausgeschaltet werden.

ACHTUNG:
Installieren Sie entweder den SAL oder die Automatische Anmeldung mit Smartcard.

Alle folgenden Anmeldungen an andere Applikationen müssen manuell erfolgen.

Die Anmeldung an Novell funktioniert nur in Verbindung mit Smartcard.

Ist die Windows-Option „Immer diesen Benutzer anmelden“ aktiviert, kann kein SAL durchgeführt werden.

17.1.1 Sicheren automatischen Logon (SAL) einschalten

Technisch gesehen funktioniert der SAL folgendermaßen: Ein Benutzer meldet sich in der Pre-Boot Authentisierung mit seinen SafeGuard Easy-Zugangsdaten an und gibt dann im Windows Anmeldedialog seine Windows-Daten ein. Der SAL stellt zwischen dem angemeldeten SafeGuard Easy-Benutzer und dem Windows-Benutzer eine Beziehung her, die in der verschlüsselten Datei `Sgsal.dat` abgespeichert wird. `Sgsal.dat` ist zu finden unter <*Systemlaufwerk*>`\SYSTEM32`. Bei einer erneuten Anmeldung in der Pre-Boot Authentisierung reicht der SAL ohne Benutzerinteraktion die Windows-Daten an den Windows-Anmeldedialog weiter.

Wollen Sie den SAL einsetzen,

1. Installieren Sie SafeGuard Easy mit
   - „Sicherem Automatischer Logon“
     ACHTUNG:
     Nicht die Option „Automatische Smartcard Anmeldung“ installieren!
   - Pre-Boot Authentisierung
2. Starten Sie Ihren Rechner neu.
3. Authentisieren Sie sich in der Pre-Boot Authentisierung mit den SafeGuard Easy-Benutzerdaten.
4. Nach der Anmeldung erscheint bei der erstmaligen Anmeldung der gewohnte Windows Logon-Dialog.
5. Füllen Sie die Eingabefelder mit den korrekten Anmeldeinformationen und drücken Sie [OK].
6. Anschließend wird der SAL-Dialog angezeigt.

SafeGuard Easy - Sicherer Automatischer Logon
SafeGuard Easy kann Sie mit den gerade gemachten Angaben automatisch an Windows anmelden, wann immer Sie sich beim Systemstart mit dem derzeitigen SafeGuard Easy Benutzer anmelden.
Wollen Sie in Zukunft automatisch an Windows angemeldet werden ?
Diesen Dialog für den angemeldeten SafeGuard Easy Benutzer nicht mehr anzeigen
Ja
Nein

[Ja]: Aktiviert die Beziehung zwischen SafeGuard Easy- und Windows Benutzer.

[Nein]: Verwendet SAL-Funktionalität nicht

Der Status des Auswahlkästchens „Diesen Dialog für den angemeldeten SafeGuard Easy Benutzer nicht mehr anzeigen.“ entscheidet, ob der Dialog bei jeder Anmeldung erneut erscheint oder nicht.

7. Drücken Sie [OK] und aktivieren Sie das Auswahlkästchen.
8. Der SafeGuard Easy-Benutzer wird mit dem Windows-Benutzer verknüpft. Beim nächsten Neustart des PC wird nach der Eingabe der SafeGuard Easy-Benutzerdaten in der Pre-Boot Authentisierung die Anmeldung an Windows automatisch durchgeführt.

Windows-Kennwort bei aktivem SAL ändern

Windows-Kennworte müssen aus Sicherheitsgründen immer wieder geändert werden. Wie ein neues Kennwort in den Sicheren automatischen Logon integriert wird, ist jedoch abhängig davon, wie es geändert wird.

- **Administrator erzwingt Kennwortänderung**

  Erzwungen wird eine Kennwortänderung im Benutzerprofil über die Option „Benutzer muss Kennwort ändern bei der nächsten Anmeldung“. Ist die Option aktiviert, wird der Benutzer durch eine System-Mitteilung dazu aufgefordert. Der SAL ist zu diesem Zeitpunkt deaktiviert.

  Diese Meldung muss mit [OK] bestätigt und im folgenden Dialog ein neues Kennwort eingegeben werden. Sobald der Benutzer das neue Kennwort bestätigt hat, wird die SAL-Datei mit den neuen Daten synchronisiert. Bei der nächsten Anmeldung werden die Windows-Benutzerdaten wieder automatisch durchgereicht.

- **Benutzer ändert Kennwort lokal**

  – Drückt der Benutzer auf seinem Desktop die Schaltflächen [STRG]+[ALT]+[ENTF], kann er sein Kennwort im Dialog *Windows Sicherheit* über „Kennwort ändern“ modifizieren. Erfolgt die Änderung auf diese Weise, findet **eine automatische Übernahme des Windows-Kennworts** in der Datei `Sgsal.dat statt`. Der Benutzer muss nach einem Neustart die Windows-Daten nicht erneut eintragen.

  – Wird das Kennwort über die Benutzerverwaltung von Windows geändert, findet **KEINE automatische Übernahme des Windows-Kennworts** statt. Der Benutzer erhält stattdessen bei der nächsten Anmeldung einen Warnhinweis, dass das Kennwort nicht gültig ist und wird aufgefordert, das neue Kennwort in den Windows Anmeldedialog einzutragen. Das Kennwort wird dann für zukünftige Anmeldungen gespeichert.

17.1.2 Anmeldung an Windows mit Smartcard (Smartcard-SAL)

ACHTUNG:
Die Anmeldung mit Smartcard findet NICHT in der Pre-Boot Authentisierung statt.

Die Smartcard-SAL-Funktion legt die PIN so auf der Karte ab, dass die Smartcard mit der Eingabe der SafeGuard Easy-Zugangsdaten in der Pre-Boot Authentisierung automatisch freigeschaltet wird. Die Windows-Anmeldedaten werden dann von der Smartcard gelesen (vorausgesetzt sie sind auf der Karte gespeichert) und ermöglichen eine Anmeldung am Betriebssystem.

Wollen Sie die Smartcard-SAL-Funktion einsetzen,

1. Installieren Sie SafeGuard Easy mit
   - „Automatischer Smartcard Anmeldung“
     ACHTUNG: Die Option „Sicherer automatischer Logon“ nicht installieren.
   - Pre-Boot Authentisierung („Passwort beim Systemstart abfragen“)
2. Starten Sie Ihren Rechner neu.
3. Authentisieren Sie sich in der Pre-Boot Authentisierung mit den SafeGuard Easy-Benutzerdaten.
4. Stecken Sie die Smartcard in den Kartenleser, erscheint der PIN-Eingabedialog. Tragen Sie dort die Benutzer-PIN ein.
5. Sind auf der Smartcard noch keine Windows-Daten vorhanden, wird ein Dialog aufgerufen mit der Frage, ob die Daten jetzt eingetragen werden sollen. Klicken Sie auf [JA], können Sie Ihre Windows-Daten (Benutzername, Passwort, Domäne) auf die Smartcard schreiben. Beachten Sie, dass der eingetragene Windows-Benutzer auch auf der Arbeitsstation angelegt ist! Andernfalls schlägt die Anmeldung fehl.

6. Anschließend wird der Dialog angezeigt, der den Smartcard-SAL ein-/ausschaltet.

   Mit Smartcard-SAL: [JA]
   Ohne Smartcard-SAL: [NEIN]

7. Beim nächsten Neustart erfolgt die Anmeldung an Windows **bei gesteckter Smartcard** automatisch nach der Eingabe der SafeGuard Easy-Benutzerdaten in der Pre-Boot Authentisierung.

Wie Sie die Smartcard-Anmeldung einem Benutzer zwingend vorschreiben, erfahren Sie im Handbuch zu SafeGuard Advanced Security im Kapitel „Token-Anmeldung Optionen“ unter „Einstellungen für Token-Anmeldung“.

Smartcard-PIN ändern bei aktivem Smartcard-SAL

PINs können mit externen SafeGuard-Tools geändert werden, z.B. mit der Token Administration.

Ändert ein Benutzer seine PIN mit diesem Tool, wirkt sich dies auf die SAL-Anmeldung per Smartcard aus, da in diesem Fall die neue und die in der `Sgsal.dat` abgelegte „alte“ PIN der Smartcard nicht mehr übereinstimmen. Bei einem Neustart stoppt das System beim PIN-Eingabedialog. Die ausgelesene „alte“ PIN produziert eine Fehlermeldung und der Benutzer wird aufgefordert, die korrekte PIN einzutragen. Trägt der Benutzer daraufhin die neue PIN ein, erfolgt die Anmeldung, und die PIN wird für zukünftige Anmeldungen gespeichert.

17.1.3 SAL/Smartcard-SAL ausschalten

Mit `CHGSAL.EXE` aus dem SafeGuard Easy-Verzeichnis können SAL und Smartcard-SAL nachträglich von einem Benutzer mit Windows-Administratorrechten deaktiviert und auch wieder eingeschaltet werden.

So aktivieren/deaktivieren Sie den SAL/Smartcard-SAL:

1. Wechseln Sie zur Eingabeaufforderung oder rufen Sie den Befehl *Ausführen* im Windows-Startmenü auf.
2. Wechseln Sie in das Verzeichnis, in dem SafeGuard Easy installiert ist. Geben Sie folgendes Kommando mit dem entsprechenden Parameter ein:

```
CHGSAL.EXE /SAL:ON | /SAL:OFF | /SCSAL:ON | /SCSAL:OFF | [ /? ]
```

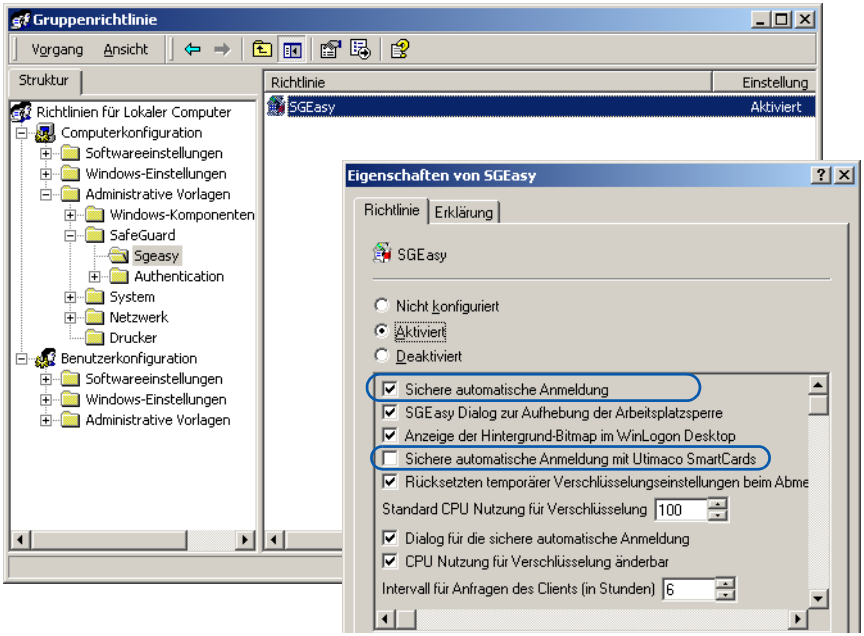
/SAL:ON	Aktiviere „Sicherer automatischer Logon“
/SAL:OFF	Deaktiviere „Sicherer automatischer Logon“
/SCSAL:ON	Aktiviere „Automatischer Smartcard Logon“
/SCSAL:OFF	Deaktiviere „Automatischer Smartcard Logon“
/?	Zeige diese Hilfe

`CHGSAL` funktioniert nur, wenn SafeGuard Easy mit SAL oder Smartcard-SAL installiert wurde.

SAL und Smartcard-SAL sind auch über eine Richtlinie in Utimacos administrativer Vorlage schaltbar. Die Richtlinie ist zu finden unter

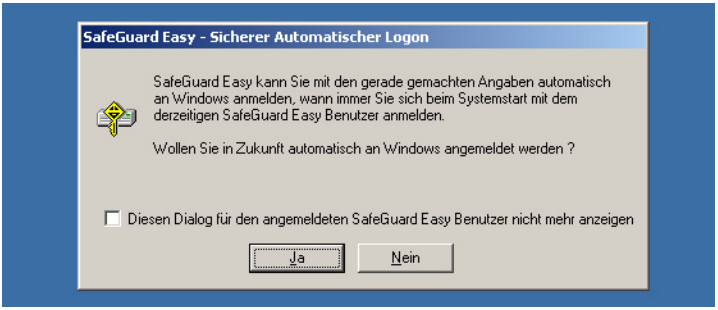
Computerkonfiguration
\Administrative Vorlagen
\SafeGuard
\SGEasy

Auf der Eigenschaftsseite von „SGEasy“ einfach den Haken vor „Sichere automatische Anmeldung“ oder „Sichere automatische Anmeldung mit Smartcards“ entfernen bzw. setzen.



17.1.4 SAL-Dialog unterdrücken

Die SafeGuard Easy SAL-Funktion meldet Benutzer automatisch an das Betriebssystem an. Aktiviert wird der SAL vom Benutzer selbst über den SAL-Dialog.

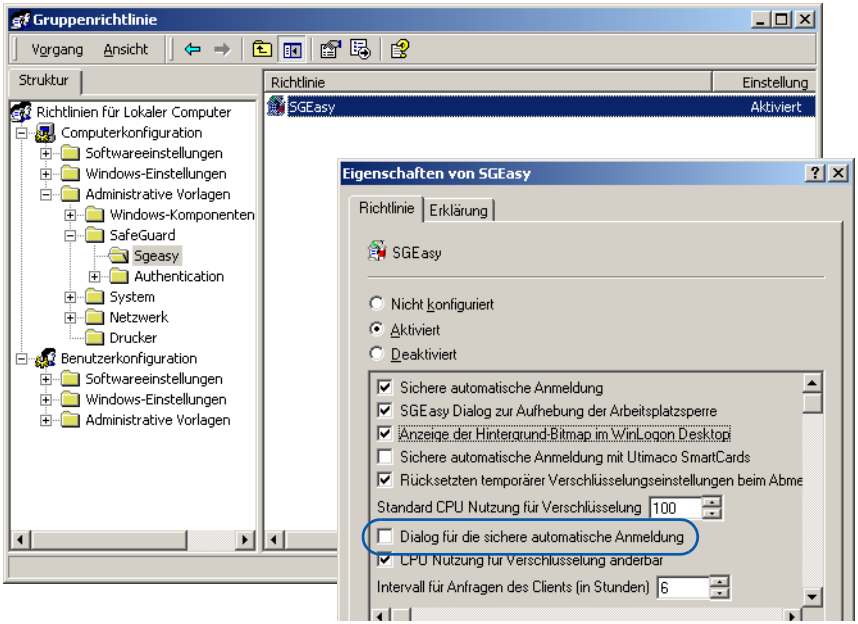

SafeGuard Easy - Sicherer Automatischer Logon
SafeGuard Easy kann Sie mit den gerade gemachten Angaben automatisch an Windows anmelden, wann immer Sie sich beim Systemstart mit dem derzeitigen SafeGuard Easy Benutzer anmelden.
Wollen Sie in Zukunft automatisch an Windows angemeldet werden ?
Diesen Dialog für den angemeldeten SafeGuard Easy Benutzer nicht mehr anzeigen
Ja
Nein

Um zu vermeiden, dass Benutzer die automatische Windows-Anmeldung ablehnen, unterdrückt SafeGuard Easy auf Wunsch den Dialog für alle SafeGuard Easy Benutzer und führt den SAL ohne Bestätigung durch.

Ausgeschaltet wird der Dialog über eine Richtlinie in Utimacos administrativer Vorlage unter

Computerkonfiguration
\Administrative Vorlagen
 \SafeGuard
  \SGEasy

Auf der Eigenschaftsseite von „SGEasy“ einfach den Haken vor „Dialog für sichere automatische Anmeldung“ entfernen.



17.1.5 SAL/Smartcard-SAL Daten löschen

Wenn Sie `Sgsal.dat` (*<Systemlaufwerk>*`\System32`) löschen, werden alle gespeicherten Benutzer-Daten entfernt. Nach einem Neustart des Rechners können Sie einem SafeGuard Easy-Benutzer neue Daten zuweisen.

Wurde ein SafeGuard Easy-Benutzer, der bereits eine Verbindung erstellt hat, auf einem System gelöscht, bleibt diese Beziehung beim erneuten Anlegen desselben Benutzers bestehen.

17.1.6 Restriktion

Der SAL ist temporär ausgeschaltet, wenn sich ein Benutzer per Challenge/Response über die Option „Einmalige Anmeldung“ anmeldet. Die „Einmalige Anmeldung“ erlaubt einem Benutzer, sich in der Pre-Boot Authentisierung von SafeGuard Easy anzumelden ohne das SafeGuard Easy-Passwort zu kennen.

Wenn nun einem Benutzer die „Einmalige Anmeldung“ in der Pre-Boot Authentisierung gestattet wurde, wird er/sie nicht automatisch an Windows angemeldet- auch wenn der SAL aktiviert ist. In diesem Fall stoppt das Betriebssystem am gewohnten Windows-Anmeldedialog und verlangt gültige Windows-Daten. Alle Aktionen werden nun unter dem Namen des angemeldeten Windows-Benutzers aufgezeichnet.

Nach jeder weiteren regulären Anmeldung mit SafeGuard Easy-Zugangsdaten in der Pre-Boot Authentisierung, wird der SAL und die automatische Windows-Anmeldung wie gewohnt ausgeführt.

17.2 Identisches Passwort für Windows und SafeGuard Easy (Passwortsynchronisierung)

Die SafeGuard Easy-Funktion „Passwortsynchronisierung“ hilft, die Wahrscheinlichkeit vergessener Passworte zu reduzieren, indem sie das Windows-Kennwort zum Passwort für SafeGuard Easy macht.

D.h. der Benutzer muss sich nur noch ein Passwort merken (nämlich das von Windows) und kann sich damit an SafeGuard Easy und das Betriebssystem anmelden.

Ist zusätzlich der Sichere automatische Logon (SAL) eingeschaltet, genügt es, das (Windows-)Passwort in der Pre-Boot Authentisierung einzutragen, die Windows-Anmeldung erfolgt automatisch.

Die Passwortsynchronisierung besitzt auch Mechanismen, die dafür sorgen, dass SafeGuard Easy-Passwort und Windows-Kennwort nach Passwortwechseln weiterhin synchron gehalten werden.

In der Grundeinstellung ist die Passwortsynchronisierung ausgeschaltet. Sie wird über einen Registry Key aktiviert.

17.2.1 Vorteile der Passwortsynchronisierung

- Benutzer müssen sich nur noch an ein Passwort (Windows-Kennwort) erinnern.
- Der Helpdesk muss nur noch ein einziges Passwort pro Benutzer verwalten.
- Die Parallelverwaltung von SafeGuard Easy- und Windows-Rechten entfällt. Bei entsprechender Konfiguration werden die Kennwortregeln allein über Windows-Richtlinien gesteuert.

17.2.2 Passwortsynchronisierung vorbereiten

So bereiten Sie die Passwortsynchronisierung vor:

1. „Sicheren automatischen Logon“ (SAL) aktivieren.
   Notwendig**,** wenn SafeGuard Easy-Benutzername und Windows-Benutzername verschieden sind.
   Nicht notwendig, wenn SafeGuard Easy-Benutzername und Windows-Benutzername identisch sind.
2. Pre-Boot Authentisierung aktivieren.
3. SafeGuard Easy Passwort-Regeln anpassen.
   Utimaco empfiehlt bei Verwendung der Passwortsynchronisierung die SafeGuard Easy-Passwortregeln weitgehend auszuschalten!
   Werden die SafeGuard Easy-Passwortregeln nicht ausgeschaltet, könnten diese mit den Windows-Kontorichtlinien kollidieren und zu Inkonsistenzen führen.

Folgende Einstellung muss zwingend in SafeGuard Easy gesetzt sein: Mindestalter der Passwörter = 0

4. Passwortsynchronisierung einschalten.
   Registry Key setzen wie unter 'Passwortsynchronisierung einschalten' beschrieben und den PC neu booten.
5. SafeGuard Easy Anmeldekomponente (Utimaco Master GINA) aktivieren.
   Bei einer SafeGuard Easy-Standardinstallation wird die Utimaco Master GINA immer installiert und muss nicht zusätzlich aktiviert werden.
   Wird die Utimaco Master GINA allerdings im Rahmen einer zentralen Verteilung von SafeGuard Easy explizit augeschaltet, ist die Passwortsynchronisierung nicht möglich.

17.2.3 Passwortsynchronisierung einschalten

Für die Aktivierung der Passwortsynchronisierung müssen Änderungen in der Windows Registrierungsdatenbank („Registry“) vorgenommen werden. Die Registrierungsdatenbank ist über den Registrierungseditor („regedit“) bzw. zentrale Mechanismen zu bearbeiten.

So schalten Sie die Passwortsynchronisierung ein:

1. Registrierungseditor („regedit“) öffnen
2. Im Registry-Zweig

   HKEY_LOCAL_MACHINE
   SOFTWARE
   Utimaco
   Sgeasy

   der DWORD-Wert-Wert „**PasswordSync**“ anlegen.
3. Den Wert von „PasswordSync“ von 0 (ausgeschaltet) auf 1 (eingeschaltet) setzen.
4. Registry verlassen und PC neu starten.

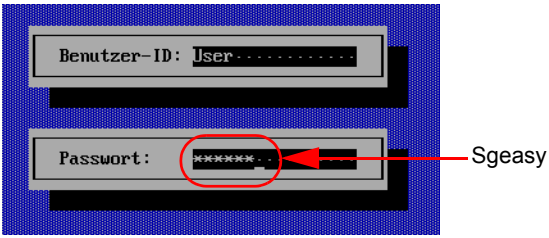
17.2.4 Passwortsynchronisierung durchführen

1. Alle Vorbereitungsmaßnahmen für Passwortsynchronisierung durchführen.

   Bitte diese SafeGuard Easy-Einstellung nicht vergessen: „Mindestalter der Passwörter“ auf den Wert „0“ setzen

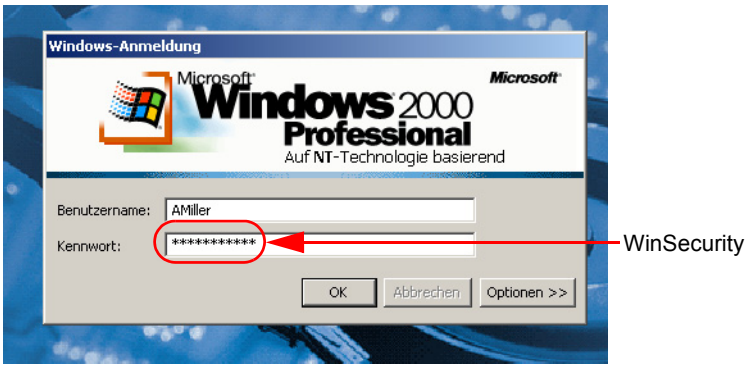
2. PC neu starten.
3. Der SafeGuard Easy-Anmeldebildschirm (Pre-Boot Authentisierung) erscheint. SafeGuard Easy-Benutzerdaten eingeben, z.B.

   SafeGuard Easy-Benutzername: **User**
   SafeGuard Easy-Passwort:**Sgeasy**

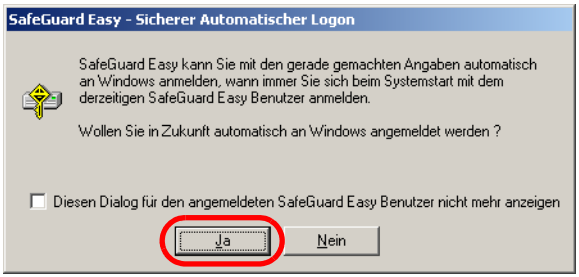


4. Der Windows-Anmeldebildschirm erscheint.
   Windows-Daten eingeben, z.B.

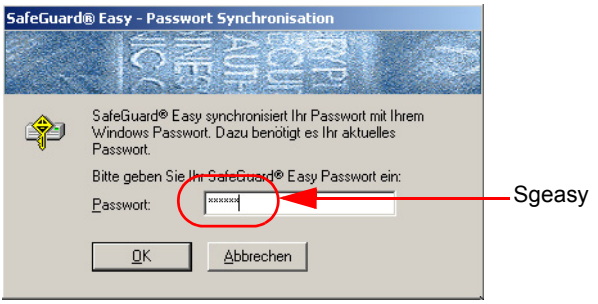
   Windows-Benutzername: **AMiller**
   Windows-Kennwort: **WinSecurity**



5. Der SAL-Dialog erscheint. Mit [JA] bestätigen.

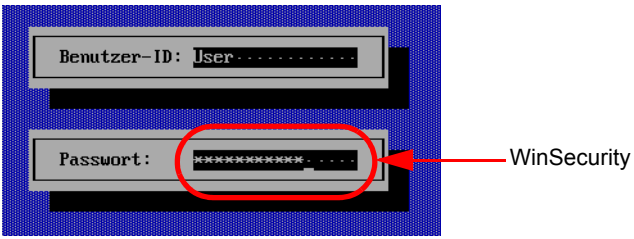

SafeGuard Easy - Sicherer Automatischer Logon
SafeGuard Easy kann Sie mit den gerade gemachten Angaben automatisch an Windows anmelden, wann immer Sie sich beim Systemstart mit dem derzeitigen SafeGuard Easy Benutzer anmelden.
Wollen Sie in Zukunft automatisch an Windows angemeldet werden ?
Diesen Dialog für den angemeldeten SafeGuard Easy Benutzer nicht mehr anzeigen
Ja
Nein

6. Der Dialog zur Passwortsynchronisierung erscheint. Hier wird das SafeGuard Easy-Passwort verlangt (in unserem Beispiel „**Sgeasy**“). Mit dem korrekten Passwort „erlaubt“ SafeGuard Easy das Synchronschalten der Passworte. Mit [OK] bestätigen.


SafeGuard® Easy - Passwort Synchronisation
SafeGuard® Easy synchronisiert Ihr Passwort mit Ihrem Windows Passwort. Dazu benötigt es Ihr aktuelles Passwort.
Bitte geben Sie Ihr SafeGuard® Easy Passwort ein:
Passwort:
OK
Abbrechen
Sgeasy

7. Der Windows-Desktop erscheint.
8. PC neu starten.
9. Die Pre-Boot Authentisierung erscheint. SafeGuard Easy-Benutzerdaten eingeben.

   SafeGuard Easy-Benutzername: **User**
   SafeGuard Easy-Passwort:**WinSecurity (= Windows-Kennwort)**



10. Der PC bootet (keine Anmeldung an Windows mehr nötig!)
11. Der Windows-Desktop erscheint.

17.2.5 Windows-Kennwort ändern bei aktiver Passwortsynchronisierung

ACHTUNG:
Auf das neue Kennwort werden die Kennwortrichtlinien von Windows angewandt und nicht die SafeGuard Easy-Regeln!

Fall 1: Benutzer ändert Windows-Kennwort lokal über den Dialog Windows Sicherheit ([Strg]+[Alt}+[Entf])

Ergebnis: Das neue Windows-Kennwort gilt sofort für Windows und SafeGuard Easy.

Fall 2: Administrator ändert Windows-Kennwort zentral oder per Fernwartung
Ergebnis: Das neue Kennwort gilt nur für Windows, aber nicht für SafeGuard Easy!

So synchronisieren Sie das „alte“ SafeGuard Easy-Passwort und das „neue“ Windows-Kennwort:

1. Nach einem Neustart trägt der Benutzer das alte Passwort an der Pre-Boot Authentisierung ein.
2. Die automatische Windows-Anmeldung schlägt fehl, da SafeGuard Easy-Passwort und Windows-Kennwort noch nicht synchronisiert wurden. Der Benutzer wird deshalb am Windows-Anmeldebildschirm aufgefordert, das neue Windows-Kennwort einzugeben.
3. Der SAL-Dialog erscheint und muss wieder mit [JA] bestätigt werden.
4. Der Dialog zur Passwortsynchronisierung erscheint. Nach Eingabe des „alten“ Passworts findet die Synchronisierung statt.
5. Nach einem Neustart des PC meldet sich der Benutzer mit dem neuen (Windows-)Passwort in der Pre-Boot Authentisierung an.

17.2.6 SafeGuard Easy-Passwort wechseln

Die Passwortsynchronisierung macht das aktuelle Windows-Kennwort immer wieder zum Passwort für SafeGuard Easy.

Utimaco rät deswegen davon ab, das SafeGuard Easy-Passwort zu ändern. Wir empfehlen zum Passwort-Wechsel die bekannten Windows-Mechanismen zu verwenden.

Ist es dennoch aus einem bestimmten Anlass nötig, das SafeGuard Easy-Passwort zu ändern, unterliegt das neue Passwort den in der SafeGuard Easy-Administration definierten Passwortregeln.

17.2.7 Dialog zur Passwortsynchronisierung abbrechen

Ob es erlaubt ist, den Dialog zur Passwortsynchronisierung unausgefüllt abzubrechen, ist per Registry Key schaltbar. Mit dieser Einstellung können z.B. Administratoren die Benutzer zwingen, die Passwortsynchronisierung durchzuführen.

Ist der Registrierungseditor geöffnet, ist unter dem Registry-Zweig

HKEY_LOCAL_MACHINE
SOFTWARE
Utimaco
Sgeasy
der DWORD-Wert „**ForcePasswordSync**“ anzulegen.

Mit dem Wert „1“ wird die „Abbrechen“-Schaltfläche ausgegraut und der Benutzer kann erst fortfahren, wenn der Sychronisationsdialog ausgefüllt ist. „0“ erlaubt, den Dialog zu überspringen.

Verlassen Sie anschließend die Registry und starten Sie den PC neu.

17.2.8 Einschränkungen

- **SafeGuard Easy beschränkt Passworte auf 16 Zeichen**
  SafeGuard Easy akzeptiert bei der Anmeldung in der Pre-Boot Authentisierung nur Passworte mit maximal 16 Zeichen.
  Diese Regel gibt SafeGuard Easy vor, und sie kann auch nicht umgangen werden. Ist ein synchronisiertes Windows-Passwort zu lang, werden für die Authentisierung in SafeGuard Easy (Pre-Boot Authentisierung, Administration etc.) die überzähligen Zeichen „abgeschnitten“.

BEISPIEL:
Windows-Kennwort (mit 20 Zeichen): „UtimacoSecurity12345“
Anmeldung in der PBA (mit 16 Zeichen): „UtimacoSecurity1“

Keine Synchronisierung erfolgt, wenn das Windows-Passwort

- den internen SafeGuard Easy-Passwortregeln widerspricht (siehe Vordefinierte Passwortregeln')
- in der SafeGuard Easy-Passworthistorie steht
- bestimmte Sonderzeichen enthält

  Erlaubt sind:
  Alle Zeichen, die mit einem Tastendruck oder in Kombination mit der SHIFT-Taste erzeugt werden, z.B.
  ! " § $ % & / ( ) = ? * ' ; : -

  Nicht erlaubt sind:
  Alle Zeichen, die über die [Alt Gr]-Taste erzeugt werden, z.B ² ³ { [ ] } \ ~ @ € | µ é è ê (und alle weiteren Buchstaben mit Accents)

  HINWEIS:
  Manche Tastaturlayouts erlauben, ein Sonderzeichen mit einem Tastendruck oder in Kombination mit der SHIFT-Taste zu erstellen, z.B. Buchstaben mit Accent auf einer französischen Tastatur. In diesem Fall akzeptiert die Passwortsynchronisierung von SafeGuard Easy das Sonderzeichen.

- **Weitere Einschränkungen bei aktivierter Passwortsynchronisierung:**

  - Nicht mehr als 16 Windows-Benutzer pro Maschine erlaubt (16 = maximale Anzahl an SafeGuard Easy-Benutzern).
  - Passwortsynchronisierung mit dem Token ist nur dann möglich, wenn der Token beim Passwortwechsel auch steckt.

17.2.9 Was tun, wenn...

... die Passwortsynchronisierung fehlschlägt und eine Fehlermeldung angezeigt wird?

Folgende Gründe sind denkbar:

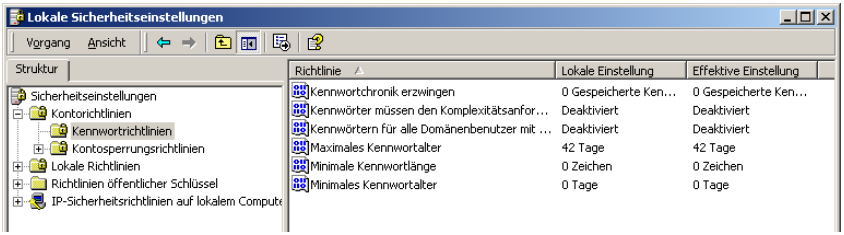
- Das synchronisierte Passwort entspricht nicht den SafeGuard Easy Passwort-Regeln (es ist z.B. zu kurz etc.)
- Das synchronisierte Passwort enthält ungültige oder von SafeGuard Easy nicht unterstützte Sonderzeichen.
- Das synchronisierte Passwort wurde laut SafeGuard Easy-Passworthistorie bereits verwendet.

Problemlösung:

Definieren Sie ein neues synchronisiertes Passwort, das nicht mit den Windows-/SafeGuard Easy-Regeln kollidiert.

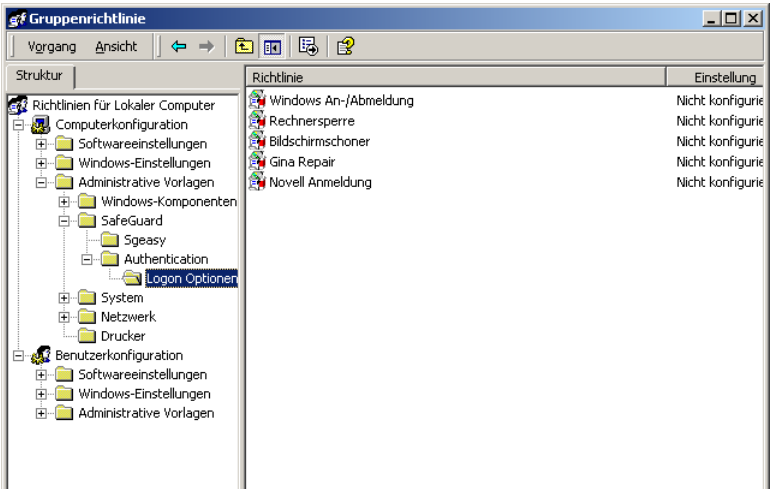
... nicht bekannt ist, wie die Richtlinien für das synchronisierte Passwort (= Windows-Kennwort) definiert werden?

Im Windows-Startmenü Einstellungen / Systemsteuerung / Verwaltung / Lokale Sicherheitseinstellungen aufrufen. Unter Kontorichtlinien > Kennwortrichtlinien sind alle möglichen Einstellungen verfügbar.



17.3 Zusätzliche Optionen für die Windows-Anmeldung

Über die mitgelieferte administrative Vorlage lassen sich bestimmte Einstellungen für die Anmeldung an das Betriebssystem zwingend vorschreiben, die man normalerweise über Windows-Einstellungen nicht beeinflussen kann.



17.3.1 Windows An-/Abmeldung

Sie finden die Richtlinie in der administrativen Vorlage unter:

Computerkonfiguration
\Administrative Vorlagen
\SafeGuard
\Authentication
\Logon Optionen
\Windows An-/Abmeldung

Die Windows An-/Abmeldung gibt Benutzern u.a. die Oberfläche vor, die bei der Anmeldung bzw. beim Sperren der Arbeitsstation auf ihrem Bildschirm erscheint.

- **Utimaco Anmeldedialog benutzen**
  Wenn Sie das Kontrollkästchen markieren, wird bei der Anmeldung der Utimaco-Anmeldedialog angezeigt. Nach Entfernen der Markierung können Sie sich über den Windows Anmeldedialog im System anmelden.

- **Utimaco Startdialog benutzen**
  Wenn Sie das Kontrollkästchen markieren, wird beim Booten der SafeGuard-Dialog *Anmeldung beginnen* angezeigt. Hier werden Sie aufgefordert [Strg] + [Alt] + [Entf] zum Öffnen des Anmeldedialogs einzugeben. Bei Entfernen der Markierung wird der entsprechende Windows Dialog angezeigt.

- **Utimaco Lockdialog benutzen**
  Wenn Sie das Kontrollkästchen markieren, wird beim Sperren der Arbeitsstation mit [Strg] + [Alt] + [Entf] der SafeGuard Lock-Dialog anstelle des Windows-Dialogs angezeigt. Nach Maus- oder Tastaturbewegungen wird der Dialog angezeigt und Sie werden aufgefordert, [Strg] + [Alt] + [Entf] zum Aufheben der Arbeitsplatzsperre einzugeben.

  Vorteil des Utimaco Lockdialogs:
  Wurde zwischen zwei korrekten Anmeldungen eine fehlerhafte Kennworteingabe registriert, wird dies im Lockdialog angezeigt. So können Sie beispielsweise kontrollieren, ob sich Unbefugte während Ihrer Abwesenheit ohne Ihr Wissen an Ihrer Arbeitsstation anmelden wollten. Bei Entfernen der Markierung wird wieder der entsprechende Windows Dialog angezeigt.

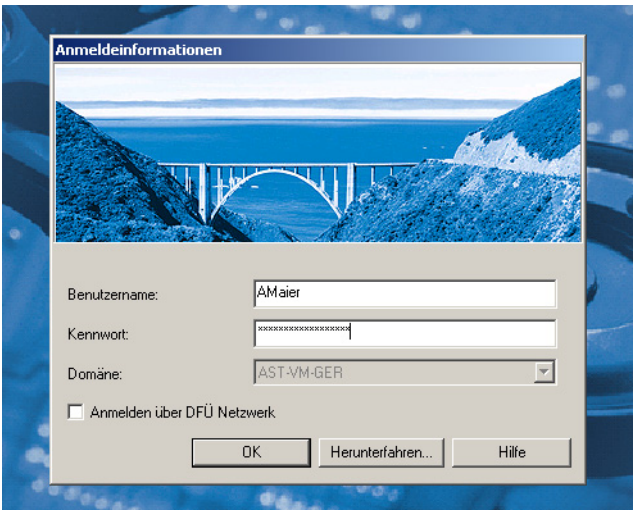
- **Vorprüfung der Benutzerdaten bei DFÜ-Anmeldung ausschalten**
  Wenn Sie das Kontrollkästchen markieren, wird beim Aufbau von DFÜ-Verbindungen keine Vorprüfung von Benutzerkonten durchgeführt.

- **Benutzerabmeldung bei gesperrter Arbeitsstation ermöglichen**
  Hat ein Benutzer eine Arbeitsstation gesperrt, können Sie anderen Benutzern das Aufheben der Sperre erlauben, wenn Sie das Kontrollkästchen markieren. Zum Aufheben der Sperre genügt die Anmeldung des anderen Benutzers.

- **Deaktivieren der DFÜ-Auswahlbox im Utimaco-Anmeldedialog**
  Wenn Sie das Kontrollkästchen markieren, wird die Option „Anmelden über das DFÜ-Netzwerk“ im Utimaco-Anmeldedialog deaktiviert.

- **SafeGuard Plugin im 3rd Party Anmeldedialog anzeigen**
  Wird diese Option aktiviert, wird auch im 3rd Party Anmeldedialog angezeigt, dass SafeGuard Authentication installiert ist.

- **Bitmap ersetzen mit**
  In diesem Eingabefeld kann ein Bitmap angegeben werden, das im Utimaco Anmelde, Start- und Lockdialog angezeigt wird, z.B. das Firmenlogo auf einen entsprechenden Hintergrund.
  Das Bitmap muss das .BMP Format haben und sich im SYSTEM32- Verzeichnis des Windows-Installationsverzeichnis befinden. Die Größe des Bitmaps ist mit 413x140 Pixel festgelegt.



17.3.2 Rechnersperre

Bei der Richtlinie „Rechnersperre“ wird festgelegt, nach wie vielen fehlgeschlagenen Anmeldeversuchen der Rechner gesperrt wird und wie sich die Wartezeit zwischen diesen Anmeldeversuchen erhöht. Der Mechanismus funktioniert nur bei Benutzern, die kein Mitglied der lokalen Gruppe der Administratoren sind.

Sie finden die Richtlinie in der administrativen Vorlage unter:

Computerkonfiguration
\Administrative Vorlagen
\SafeGuard
\Authentication
\Logon Optionen
\Rechnersperre

- **Anmelde-Fehlversuche (Standard: 3)**
  In diesem Feld bestimmen Sie die Anzahl der Anmelde-Fehlversuche eines Benutzers, der sich mit einem ungültigen Benutzernamen bzw. Kennwort anmeldet. Geben Sie beispielsweise „3“ ein, wird der Rechner gesperrt, wenn der Benutzer bei der Anmeldung dreimal hintereinander seinen Benutzernamen oder sein Kennwort falsch eingibt.
  Minimaler/Maximaler Wert: 0-999

- **Verzögerung in Sekunden (Standard: 10)**
  Tragen Sie hier den Basiswert ein, der multipliziert mit dem „Multiplikator“ die Wartezeit nach dem ersten fehlgeschlagenen Anmeldeversuch ergibt. Bei einem weiteren Fehlversuch wird die Wartezeit des vorherigen Fehlversuches als Basiswert genommen. Die Standardeinstellung ist „10“.
  Minimaler/Maximaler Wert: 0-999

- **Multiplikator (Standard: 3)**
  Der Multiplikator wird mit der Zeitbasis Verzögerung in Sekunden multipliziert. Die Standardeinstellung ist „3“.
  Minimaler/Maximaler Wert: 0-99

- **Deaktiviere STRG+ALT+Entf, wenn Computer gesperrt ist (Standard: Aktiviert)**
  Die Rechnersperre kann bei einer Anmeldung mit Token nicht mit [STRG] + [ALT] + [Entf] aufgehoben werden.

BEISPIEL:
Verzögerung von 10 Sekunden und Multiplikator von 5:
1. Fehlversuch: 50 Sekunden Wartezeit (10 * 5)
2. Fehlversuch: 250 Sekunden Wartezeit (50 * 5)
3. Fehlversuch: 1250 Sekunden Wartezeit (250 * 5)

Die Rechnersperre kann durch Neustart des Rechners und durch Anmeldung eines lokalen Administrators aufgehoben werden. Beachten Sie in diesem Zusammenhang auch die Benutzersperre von Windows.

17.3.3 Bildsschirmschoner

Ist auf einer Arbeitsstation festgelegt, dass ein Bildschirmschoner nach einer bestimmten Zeit starten soll, können Sie bestimmen, wie das System nach einem definierten Zeitraum auf dessen Aktivierung reagieren soll.

Die Einstellungen sind nur wirksam, wenn der Windows-Bildschirmschoner auch aktiviert ist!

Sie finden die Richtlinie in der administrativen Vorlage unter:

Computerkonfiguration
\Administrative Vorlagen
 \SafeGuard
  \Authentication
   \Logon Optionen
    \Bildschirmschoner

- **Aktionen (Standard: Deaktiviert)**
  Folgende Aktionen stehen zur Verfügung, die nach Einsetzen des Bildschirmschoners und der definierten Aktionsverzögerung ausgeführt werden können. Abhängig davon, ob sie für eine lokale Arbeitsstation bzw. einen Server oder eine Terminal Server Session definiert werden, wirken sich die Aktionen verschieden aus. Um die Aktionen für Terminal Server Sessions zu definieren, müssen Sie auf dem Terminal Server vorgenommen werden.

  A) Benutzer abmelden
  Der aktuelle Benutzer wird abgemeldet. Es können sich nun (auch) andere auf der Arbeitsstation oder im Netzwerk registrierte Benutzer anmelden.

  B) Computer herunterfahren
  Der PC wird automatisch heruntergefahren und muss für eine weitere Arbeitssitzung neu gestartet werden.
  In einer Terminal Server Session wird der Benutzer abgemeldet.

  C) Computer neu starten
  Es erfolgt ein automatischer Neustart. In einer Terminal Server Session wird der Benutzer abgemeldet.

  D) Computer in Ruhezustand versetzen
  Der Computer wird in den Ruhezustand versetzt.
  In einer Terminal Server Session wird die Session gesperrt.

  HINWEIS:
  Sind auf dem System SafeGuard Advanced Security und SafeGuard Easy installiert, funktioniert die Option „Computer in Ruhezustand“ versetzen nur, wenn die Version SafeGuard Easy 4.0 oder höher verwendet werden.

  E) Verbindung trennen
  Hat auf einer lokalen Arbeitsstation keine Auswirkung.
  In einer Terminal Server Session wird die Verbindung getrennt.

F) Standby
Der Computer wird in den Standby-Modus versetzt.
In einer Terminal Server Session wird die Session gesperrt.

Überblick über mögliche Aktionen und ihre Auswirkungen auf den lokalen Rechner bzw. auf die Terminal Server Session:

Einstellung	**Aktion lokal bzw. auf Server**	**Aktion in Terminal Server Session**
<Keine>	keine	keine
Benutzer abmelden	abmelden	abmelden
Computer herunterfahren	herunterfahren	abmelden
Computer neu starten	neu starten	abmelden
Computer in Ruhezustand versetzen	in Ruhezustand versetzen	Session sperren
Verbindung trennen	keine	Verbindung trennen
Standby	Standby	Session sperren

HINWEIS:
In einer **Remote Desktop Session** gelten für die Einstellungen dieselben Aktionen wie sie für **lokal bzw. auf dem Server** beschrieben sind.

- **Aktionsverzögerung (Standard: 15)**
  Mit Aktionsverzögerung stellen Sie den Zeitraum (in Minuten) ein, nach dem das System eine der beschriebenen Aktionen ausführen soll. Als Standardwert ist 15 vorgegeben. Sie können die Zahl entweder direkt per Tastatureingabe oder mit den Richtungspfeilen ändern.
- **Bildschirmschoner sperren (Standard: Deaktiviert)**
  Ein gestarteter Bildschirmschoner wird in der Regel mit einer Mausbewegung oder Tastatureingabe aufgehoben und der Benutzer kann ohne Eingabe seiner Zugangsdaten weiterarbeiten. Ist das Kontrollkästchen „Bildschirmschoner sperren“ aktiviert, wird die Arbeitsstation gesperrt. Der Zugriff auf die Arbeitsstation ist erst wieder nach korrekter Eingabe der Zugangsdaten möglich.

BEISPIEL:

Auf den Arbeitsstationen ist definiert, dass der Bildschirmschoner zehn Minuten nach der letzten Benutzeraktion (Tastatureingabe, Mausbewegung) einsetzen soll. Haben Sie als auszuführende Aktion ´Computer herunterfahren´ gewählt und als Aktionsverzögerung den Wert 13 eingegeben, wird der PC 23 Minuten nach der letzten Aktion am Arbeitsplatz automatisch heruntergefahren.

17.3.4 Authentisierungsmodul (GINA) reparieren

Utimaco besitzt eine eigene Anmeldekomponente, die Utimaco Master GINA (`SGGINA.dll`). Die Utimaco Master GINA wird nach der Installation eines Utimaco-Produkts als Erste in der GINA-Kette platziert und kontrolliert damit den Anmeldemechanismus. Die Installation anderer Produkte kann die Reihenfolge der aufgerufenen Anmeldekomponenten ändern.

Sie finden die Richtlinie in der administrativen Vorlage unter:

Computerkonfiguration
\Administrative Vorlagen
\SafeGuard
\Authentication
\Logon Optionen
\GINA Repair

- **Automatische Korrektur der Aufrufsequenz (Standard: Aktiviert)**
  Stellt sicher, dass die Utimaco Master GINA automatisch an der ersten Stelle der GINA-Kette platziert wird.

- **Verhalten bei unbekannten GINAs**

  Benutzer fragen
  Beim erstmaligen Initialisieren wird in einem Dialog gefragt, ob die unbekannte oder die original Microsoft GINA verwendet werden soll. Wird in diesem Dialog die Checkbox bei „Diese Meldung nicht mehr anzeigen“ aktiviert, wird die Benutzerreaktion in der Registrierung gespeichert und beim nächsten Neustart dieser Wert verwendet.

  Original Microsoft GINA verwenden
  Die Original Microsoft GINA wird an die erste Stelle der GINA-Kette platziert.

  Unbekannte GINA verwenden
  Platziert die unbekannte GINA an die erste Stelle der GINA-Kette.

17.3.5 Novell Anmeldung

Gilt nur für Single Sign On von SafeGuard Advanced Security!

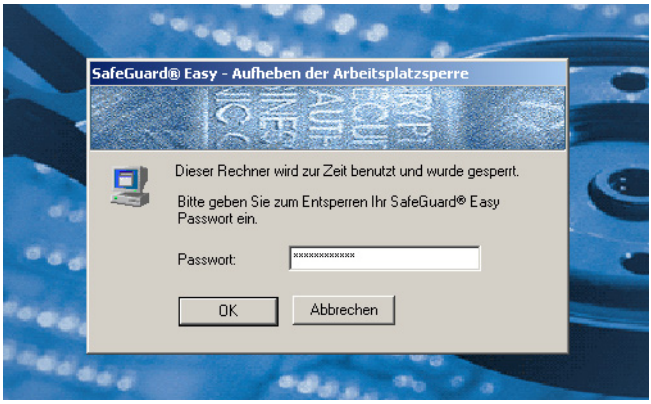
Werden mehrsprachige Novell Versionen eingesetzt, sucht SafeGuard Single Sign On den Standard-Eintrag und den im Feld „Titel des Anmeldedialogs" eingetragenen Anmeldedialog und befüllt diesen mit den auf dem Token gespeicherten Novell-Anmeldeinformationen.

Sie finden die Richtlinie in der administrativen Vorlage unter:

Computerkonfiguration
\Administrative Vorlagen
\SafeGuard
\Authentication
\Logon Optionen
\Novell Anmeldung

18 Arbeitsplatzsperre von SafeGuard Easy

SafeGuard Easy ersetzt die reguläre Windows-Arbeitsplatzsperre mit einem eigenen Dialog.


SafeGuard® Easy - Aufheben der Arbeitsplatzsperre
Dieser Rechner wird zur Zeit benutzt und wurde gesperrt.
Bitte geben Sie zum Entsperren Ihr SafeGuard® Easy Passwort ein.
Passwort:
****
OK
Abbrechen

Wenn der PC sich im Pausenmodus befindet, kann nur der Benutzer, der ihn gesperrt hatte, durch **Eingabe seines SafeGuard Easy Passworts** die Arbeitsoberfläche wieder aktivieren.

Bildschirm und Arbeitsoberfläche werden gesperrt

- nach Drücken von [Strg]+[Alt]+[Entf] und [Computer sperren]
- nach Ablauf einer eingestellten Zeit ohne Bedienung (Wartezeit)
- durch Ziehen des Token

Für die Arbeitsplatzsperre erscheint dasselbe Hintergrundbild wie während der Anmeldung, dieses kann aber geändert werden (siehe 'Hintergrund-Bitmap in der Windows-Anmeldung austauschen').

18.1 Voraussetzungen

Die Arbeitsplatzsperre funktioniert nur, wenn

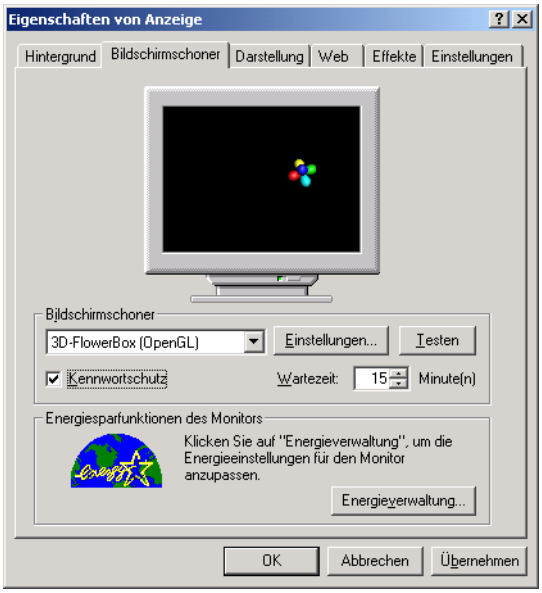
- die Pre-Boot Authentisierung aktiviert ist
- der Benutzer über den SAL automatisch an das Betriebssystem angemeldet wurde.
- der Windows-Bildschirmschoner mit Kennwortschutz eingeschaltet ist

Nachträglich ausgeschaltet wird die SafeGuard Easy Arbeitsplatzsperre, wenn sich ein Benutzer nach erfolgreicher Anmeldung von Windows abmeldet und wieder anmeldet.

18.2 Windows-Bildschirmschoner mit Kennwortschutz aktivieren

Die SafeGuard Easy-Arbeitsplatzsperre wird in den Windows-Einstellungen über Programme / Systemsteuerung / Anzeige / Bildschirmschoner gesteuert.

Der PC muss nach Konfigurieren des Windows-Bildschirmschoners neu gestartet werden!



Es muss zunächst ein Bildschirmschoner ausgewählt werden, danach die Optionen „Kennwortschutz“ und „Wartezeit“ angepasst werden.

- **Kennwortschutz**
  Erzwingt die Abfrage des SafeGuard Easy-Passworts, muss aktiviert werden.

- **Wartezeit**
  Gibt die Zeit (in Minuten) an, die ohne Bedienung des Arbeitsplatzes vergehen muss, bis die Arbeitsplatzsperre aktiviert wird.

  Wenn Sie hier 15 einstellen, würde der Bildschirm nach 15 Minuten ohne Tastatureingabe oder Mausbedienung gesperrt.
  Der Benutzer muss sich zur Fortsetzung seiner Arbeit erneut mit dem SafeGuard Easy Passwort anmelden.

Um den Arbeitsplatz vor unbefugten Benutzern zu schützen, schalten Sie bitte die Arbeitsplatzsperre ein.

18.3 SafeGuard Easy Arbeitsplatzsperre nicht anzeigen

Es besteht die Möglichkeit, die SafeGuard Easy-Arbeitsplatzsperre auszuschalten und stattdessen den regulären Windows-Dialog anzuzeigen.

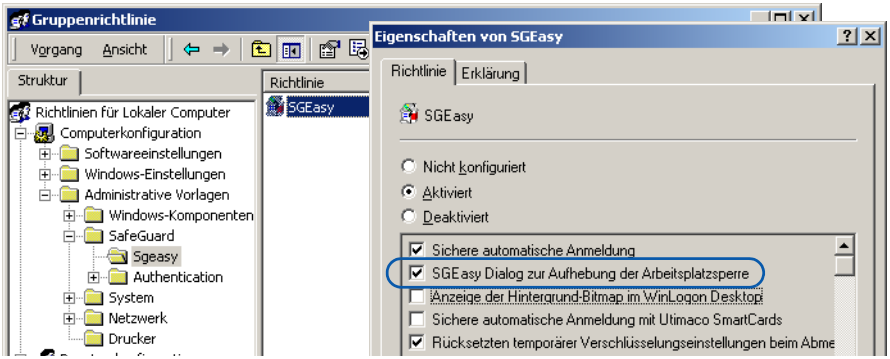
> ***ACHTUNG:***
> Der reguläre Windows-Dialog wird nicht mit dem SafeGuard Easy-Passwort, sondern mit dem Windows-Kennwort aufgesperrt.
> Der SafeGuard Easy-Passwortschutz für die Arbeitsplatzsperre ist damit nicht mehr gegeben!

Über die mitgelieferte administrative Vorlage lässt sich unter der Richtlinie „SGEasy Dialog zur Aufhebung der Arbeitsplatzsperre“ (Haken vor der Richtlinie entfernen) die SafeGuard Easy Arbeitsplatzsperre deaktivieren.

Sie finden die Richtlinie unter

Computerkonfiguration
\Administrative Vorlage
\SafeGuard
\Sgeasy

Nach einem Logoff ist die Einstellung wirksam.



19 Sicheres Wake On LAN

Der Wake On LAN-Modus (im folgenden WOL) von SafeGuard Easy ist der sicherste Weg, um die Vorteile von Wake On LAN mit dem Schutz des PCs durch Festplattenverschlüsselung zu kombinieren. SafeGuard Easys WOL erlaubt zu diesem Zweck, die Pre-Boot Authentisierung für eine definierte Anzahl von Neustarts auszuschalten und danach wieder zu aktivieren, um z.B. neue Software zu verteilen. Währenddessen ist es jedoch nicht möglich, die inaktive Pre-Boot Authentisierung zu nutzen und sich über eine geglückte Windows-Anmeldung ins System einzuschleichen.

WOL ist ein optimaler Kompromiss zwischen Pre-Boot-Schutz und dem Ausführen zentral gesteuerter Aufgaben.

19.1 Überblick

Generell ermöglicht Wake on LAN, einen Rechner im lokalen Netzwerk von einem zweiten Rechner aus einzuschalten, um z.B. neue Softwareupdates einzuspielen oder generelle Wartungsarbeiten durchzuführen.

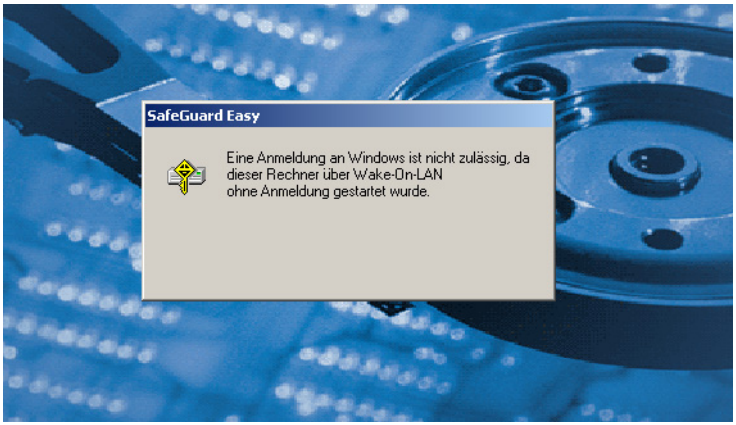
Das bequeme Ausführen zentraler Aufgaben auf mit SafeGuard Easy gesicherten Rechnern scheitert in Versionen kleiner 4.0 an der Pre-Boot Authentisierung, da der Rechner an der Pre-Boot Authentisierung (wenn vorhanden) stoppt und die Eingabe der SafeGuard Easy-Zugangsdaten erwartet. In diesem Fall startet das Betriebssystem nicht und baut somit keine Netzwerkverbindung auf, was dazu führt, dass die Ausführung zentral gesteuerter Aufgaben fehl schlägt.

Die neue WOL-Technik in SafeGuard Easy ermöglicht dem Administrator, den SafeGuard Easy-Clients eine Anzahl von Neustarts zu erlauben, bevor automatisch wieder die Pre-Boot Authentisierung aktiv wird. Wenn etwa die Anzahl der Automatischen Anmeldungen auf „3“ gesetzt wird, startet der PC dreimal in Folge mit ausgeschalteter Pre-Boot Authentisierung, beim vierten Neustart wird die Pre-Boot Authentisierung wieder angezeigt (vorausgesetzt, sie ist eingeschaltet).

Während der n-maligen Bootphase wird die Windows-Anmeldung unterdrückt. Der Rechner bootet selbsttätig und das automatische Softwareupdate kann über das Netzwerk durchgeführt werden.

19.2 Sperre der Windows-Anmeldung

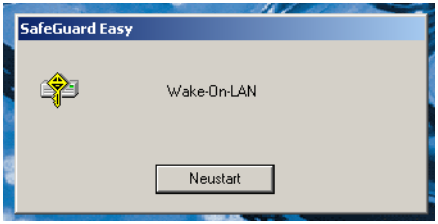
Im Wake On LAN Modus ist der Rechner gegen lokale Windows-Benutzeranmeldungen gesichert. Es erscheint statt des gewohnten Windows-Anmeldedialogs die Wake On LAN-Meldung ("Eine Anmeldung an Windows ist nicht zulässig, da dieser Rechner über Wake-On-LAN ohne Anmeldung gestartet wurde.")


SafeGuard Easy
Eine Anmeldung an Windows ist nicht zulässig, da dieser Rechner über Wake-On-LAN ohne Anmeldung gestartet wurde.

Die Sperre der Windows-Anmeldung im WOL-Modus funktioniert nur, wenn die SafeGuard-Anmeldekomponente (Utimaco Master GINA) installiert ist!

19.3 Wake On LAN-Meldung anpassen

Die WOL-Meldung („Eine Anmeldung an Windows ist nicht zulässig ... “) kann mit Standard Windows-Mechanismen (Registry-Einträge) zentral angepasst werden.



Neustart-Schaltfläche einfügen

Die Schaltfläche "Neustart" wird im Dialog eingefügt, wenn folgender Registry Key [DWORD-Wert] auf „0“ gesetzt wird:

HKEY_LOCAL_MACHINE
SOFTWARE
Utimaco
SGEasy
WOLDisableShutdown

Meldungstext ändern

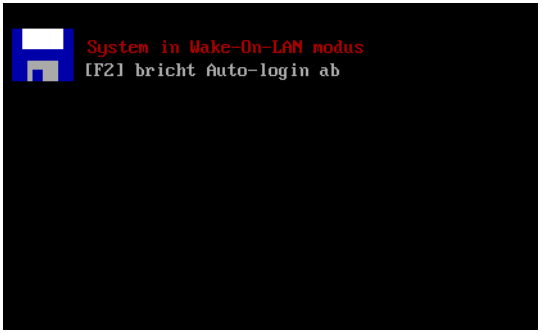
Ein neuer Meldungstext erscheint, wenn unter folgendem Registry Key [Zeichenfolge] ein neuer Text eingegeben wird:

HKEY_LOCAL_MACHINE
Software
Utimaco
SGEasy
WOLNotice

19.4 Wake On LAN Sperre temporär aufheben

Wenn Benutzer trotz WOL Modus ihren PC nutzen müssen, gibt es eine Möglichkeit, die Sperre zeitweise aufzuheben:

In der Pre-Boot Phase erscheint in der linken, oberen Monitorecke ein Diskettensymbol für ca. 5 Sekunden.



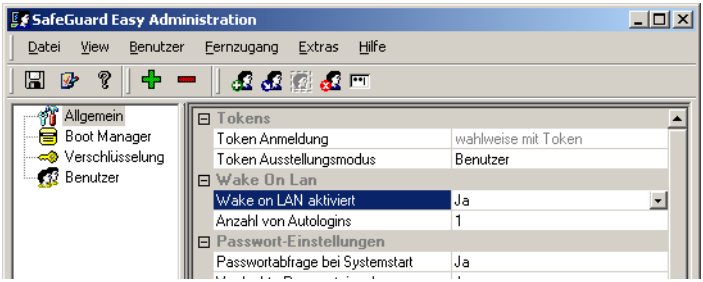
Wird während dieser Zeit [F2] gedrückt, erscheint die Pre-Boot Authentisierung und der Benutzer kann sich wie gewohnt mit gültigen SafeGuard Easy-Zugangsdaten und später an Windows anmelden. Dass der Rechner sich im Wake On LAN Modus befindet, sieht der Benutzer an einer über [F2] blinkenden Warnung.

Wird der PC über den abgesicherten Modus gestartet ([F8] während des Bootvorgangs drücken), ermöglicht die eingebaute SafeGuard-Sperre, dass sich nur Benutzer mit Windows-Administratorrechten im abgesicherten Modus anmelden können.

19.5 Wake on LAN konfigurieren

WOL wird in der Regel in größeren IT-Umgebungen und nicht für Standalone PCs eingesetzt. Der Administrator erstellt eine Konfigurationsdatei mit den entsprechenden WOL Einstellungen und verteilt diese an die Clients im Unternehmen.

Konfiguriert wird SafeGuard Easys Sicheres Wake-On LAN in den Verwaltungsprogrammen über die Konfigurationsseite „Allgemein“.



Folgende Einstellungen sind möglich:

- **Wake on LAN aktiviert**:
  Schaltet Wake On LAN Modus ein/aus.

- **Anzahl Automatischer Anmeldungen** (Standard: 1):
  Definiert die Anzahl der Neustarts mit ausgeschalteter Pre-Boot Authentisierung, wenn Wake On LAN eingeschaltet ist.

  Utimaco empfiehlt, immer **einen Neustart mehr als notwendig zu erlauben**, um unvorhergesehene Probleme zu umgehen.

Sobald die Konfigurationsdatei an die Benutzer-PCs verteilt wurde, startet der PC nun n-Mal ohne Pre-Boot Authentisierung neu. Nach Ablauf der definierten Anzahl an Neustarts ohne Pre-Boot Authentisierung erscheint wie gewohnt die Pre-Boot Authentisierung und verlangt nach den korrekten SafeGuard Easy-Benutzerdaten.

20 Ruhezustand (Hibernation)

Die Windows-Funktion „Ruhezustand“ wird von Benutzern mit mobilen Geräten gerne genutzt, um den Arbeitsvorgang temporär zu unterbrechen. Wird etwa ein Notebook bei aktiviertem Ruhezustand im laufenden Betrieb zugeklappt, schaltet sich das Gerät automatisch aus und stellt nach einem Neustart wieder exakt die Bildschirmoberfläche der letzten Sitzung her.

Zur Sicherung der Daten im Ruhezustand hat SafeGuard Easy hier eine besondere Lösung, die nicht jedes Verschlüsselungsprodukt bietet.

20.1 Überblick

Im Ruhezustand wird der Inhalt des Arbeitsspeichers (RAM) in die Systemdatei Hiberfile.sys im Hauptverzeichnis der Betriebssystempartition (i.d.R. Laufwerk C) geschrieben und auf der Festplatte gespeichert. Die Größe der Hiberfile.sys entspricht in etwa der Größe des zur Verfügung stehenden Arbeitsspeichers. Anschließend wird der Computer ausgeschaltet. Wenn Sie den Computer wieder einschalten, wird der Desktop genau so wiederhergestellt, wie Sie ihn beim Herunterfahren verlassen haben (d.h. der Inhalt der Hiberfile.sys wird wieder zurück in den Arbeitsspeicher geschrieben). Nach der Deaktivierung des Ruhezustandes wird die Hiberfile.sys ungültig gemacht.

20.2 Ruhezustand und SafeGuard Easy

Auf einer unverschlüsselten Betriebssystempartition ist das Umschalten des Rechners in den Ruhezustand ein Sicherheitsrisiko, weil dabei der komplette Hauptspeicherinhalt ausgelagert wird und für nicht autorisierte Dritte leicht zugänglich ist.

Auf einer verschlüsselten Betriebssystempartition erlaubt es SafeGuard Easy, den Ruhezustand zu nutzen und die erzeugte Hiberfile.sys verschlüsselt und damit sicher auf der Platte abzulegen. Somit sind alle Daten auf der Festplatte zu jeder Zeit verschlüsselt. Zugriff auf das System erhalten nur Benutzer, die sich nach einem Wiederanlauf des Rechners in der Pre-Boot Authentisierung (vorausgesetzt, diese ist aktiviert) mit gültigen SafeGuard Easy-Zugangsdaten authentisieren können.

HINWEIS:
Wenn sich unterschiedliche SafeGuard Easy-Benutzer eine Arbeitsstation teilen, gelangt trotz Authentisierung mit unterschiedlichen SafeGuard Easy-Zugangsdaten in der Pre-Boot Authentisierung jeder von ihnen in das Profil des SafeGuard Easy-Benutzers, der den Ruhezustand initiiert hat.

In diesem Fall ist es möglich, beim Wiederanlauf des Rechners das Windows-Kennwort anzufordern (Energieoptionen / Erweitert / Kennwort beim Reaktivieren des Computers anfordern). Diese Einstellung zwingt die Benutzer, sich zusätzlich mit ihren Windows-Daten anzumelden (Nachteil: zweifache Authentisierung).

20.3 Voraussetzungen und Restriktionen

Das Zusammenspiel von SafeGuard Easy und dem Ruhezustand funktioniert unter folgenden Voraussetzungen:

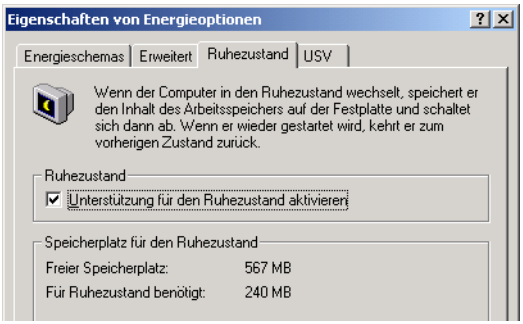
Ruhezustand mit SafeGuard Easy unterstützt ...	Ruhezustand mit SafeGuard Easy unterstützt NICHT ...
Windows 2000 und Windows XP	
Festplattenlaufwerke (Microsoft IDE, Serial-ATA, SCSI), die Microsoft Standardschnittstellen benutzen; bei Serial-ATA können bei manchen Geräten Probleme auftreten, wenn die Standardschnittstellen nicht benutzt werden.	Festplattentreiber von Drittherstellern
die SafeGuard Easy-Verschlüsselungsmodi „Standard“ und „Partitionierung“	den SafeGuard Easy-Verschlüsselungsmodus „Bootschutz“

HINWEIS:
Bei der Verwendung von externen Geräten oder Einsteckkarten (Soundkarten etc.) bitte prüfen, ob diese die Microsoft Energieverwaltung unterstützen und der Rechner auch ohne SafeGuard Easy problemlos in den Ruhezustand versetzt/aus dem Ruhezustand zurückgeholt werden kann.

20.4 Ruhezustand einrichten

Für die bestmögliche Sicherheit bei Aktivierung des Ruhezustands empfehlen wir folgende Konfiguration:

1. Rufen Sie im Windows Startmenü nacheinander Einstellungen / Systemsteuerung / Energieoptionen auf. In Registerkarte *Ruhezustand* aktivieren Sie die Checkbox „Unterstützung für Ruhezustand“.


Eigenschaften von Energieoptionen
Energieschemas
Erweitert
Ruhezustand
USV
Wenn der Computer in den Ruhezustand wechselt, speichert er den Inhalt des Arbeitsspeichers auf der Festplatte und schaltet sich dann ab. Wenn er wieder gestartet wird, kehrt er zum vorherigen Zustand zurück.
Ruhezustand
Unterstützung für den Ruhezustand aktivieren
Speicherplatz für den Ruhezustand
Freier Speicherplatz: 567 MB
Für Ruhezustand benötigt: 240 MB

2. Wenn sich zwei Benutzer einen SafeGuard Easy-Rechner teilen, aktivieren Sie in der Registerkarte *Erweitert* im Feld Optionen „Kennwort beim Reaktivieren des Computers anfordern“.
3. Starten Sie die SafeGuard Easy Administration.
4. Aktivieren Sie die Pre-Boot Authentisierung (wenn noch nicht geschehen) unter Allgemein / Passworteinstellungen / Passwortabfrage beim Systemstart.
5. Verschlüsseln Sie mindestens die Betriebssystempartition über Verschlüsselung / Laufwerke / Festplattenlaufwerke.

   Zum Schutz Ihres Systems empfehlen wir, zusätzlich zur Betriebssystempartition ihre kompletten Datenpartitionen zu verschlüsseln.

21 Disketten- und Geräteverschlüsselung schalten

Um eine Arbeitsstation optimal abzusichern, ist es ratsam, die Disketten- und Geräteverschlüsselung von SafeGuard Easy einzuschalten. Manche Situationen erfordern allerdings ein flexibles Handhaben des Verschlüsselungsmechanismus.

SafeGuard Easy ermöglicht, die Verschlüsselung von Disketten- und Wechselmedienlaufwerken ein- bzw. auszuschalten und für die Dauer einer Anmeldung eigene Schlüssel zu definieren. Die temporären Einstellungen werden nach der Abmeldung des angemeldeten Windows-Benutzers wieder zurückgesetzt, und es gelten wieder die Systemeinstellungen.

Voraussetzung für das zeitweilige Wechseln der Verschlüsselungseinstellungen ist, dass eine Authentisierung mit SafeGuard Easy-Benutzerdaten in der Pre-Boot Authentisierung stattgefunden hat und die Verschlüsselung für Disketten/Wechselmedien aktiviert ist.

Um Probleme zu vermeiden, beachten Sie bitte Hinweise zur Disketten- und Geräteverschlüsselung'.

21.1 Notwendige SafeGuard Easy-Rechte

Voraussetzung für das Schalten der Verschlüsselung ist, dass der Benutzer über die entsprechenden SafeGuard Easy-Rechte verfügt. Ob ein Benutzer die Verschlüsselung von Disketten- oder Wechselmedienlaufwerken schalten darf, wird in den SafeGuard Easy-Benutzereinstellungen unter dem Punkt „Rechte“ definiert (siehe 'Benutzerrechte').

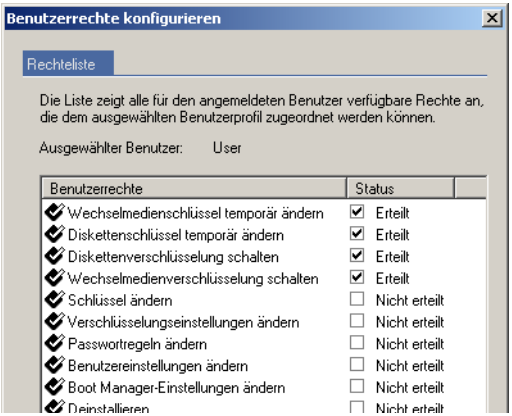
Folgende Benutzerrechte sind nötig:

- **Für das Schalten der Verschlüsselung:**

  - Diskettenverschlüsselung schalten
  - Wechselmedienverschlüsselung schalten

- **Für das Setzen eines temporären Schlüssels:**

  - Diskettenschlüssel temporär ändern
  - Wechselmedienschlüssel temporär ändern



21.2 Verschlüsselung schalten

Der Verschlüsselungsstatus wird über den Windows Explorer geschaltet. SafeGuard Easy erweitert dazu das Windows Explorer-Kontextmenü um den Eintrag „Verschlüsselung“.

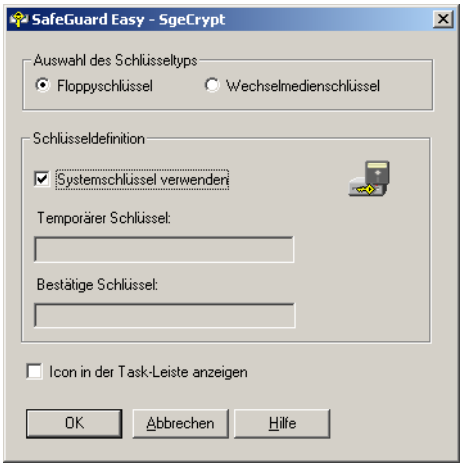
Wenn Sie mit der rechten Maustaste auf ein verschlüsseltes Laufwerk klicken, wird ein Kommando zum Einschalten/Ausschalten der Verschlüsselung eines Disketten- oder Wechselmedienlaufwerks angezeigt.

HINWEIS:
Der Verschlüsselungsstatus kann für jedes Wechselmedienlaufwerk einzeln eingestellt werden!

21.3 Schlüssel setzen mit SgeCrypt

Neue Schlüssel werden für die Dauer einer Anmeldung über das Tool SGECRYPT vergeben.

Um SGECRYPT zu öffnen, wählen Sie nacheinander Programme / Utimaco / SafeGuard Easy / **Disketten- und Geräteverschlüsselung schalten**.



Sie können aus den folgenden Optionen wählen:

- **Auswahl des Schlüsseltyps**
  Bestimmt, ob der Schlüssel für Diskette oder Wechselmedien gelten soll.

- **Systemschlüssel verwenden**

  Aktiviert:
  Der auf der Arbeitsstation (beispielsweise während der Installation) für Disketten oder Wechselmedienlaufwerke voreingestellte Schlüssel wird verwendet.

  Deaktiviert:
  Ein neuer Schlüssel wird verwendet.

Um einen Systemschlüssel wählen zu können, muss dieser auch auf der Arbeitsstation eingestellt sein. Ist dies nicht der Fall, kann ein Benutzer mit entsprechenden Rechten in der Administration im nachhinein diesen Systemschlüssel setzen.

- **Temporärer Schlüssel**
  Der temporäre Schlüssel gilt nur für die Dauer einer Arbeitssitzung. Nach dem Neustart wird er wieder entfernt, und der Systemschlüssel wird wieder aktiv.

- **Icon in der Task-Leiste anzeigen**
  Zeigt in der Taskleiste ein Icon an, über das dieser Dialog aufgerufen werden kann. Die Einstellung ist nur für den aktuell angemeldeten Benutzer gültig. Es sind keine Windows-Administratorrechte nötig, um das Icon anzuzeigen/nicht anzuzeigen.

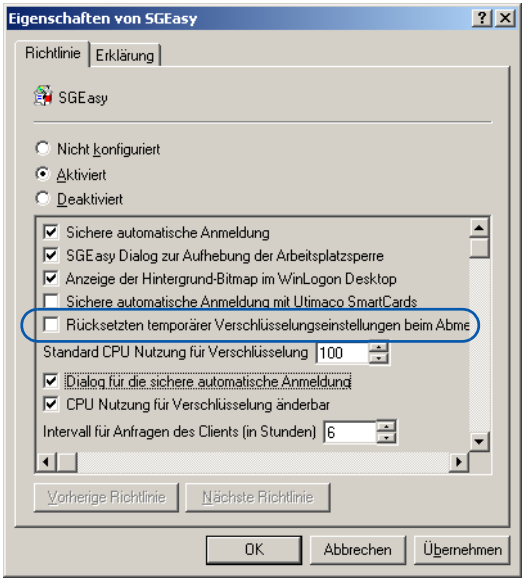
21.3.1 Temporäre Schlüssel nicht zurücksetzen

Wenn die temporären Schlüsseleinstellungen auch nach einem Neustart gelten sollen, ist dies über eine Richtlinie in Utimacos administrativer Vorlage konfigurierbar (siehe 'Häufig verwendete Registry-Einstellungen für SafeGuard Easy über die administrative Vorlage ändern').

Sie finden die Richtlinie unter

Computerkonfiguration
\Administrative Vorlagen
 \SafeGuard
  \SGEasy

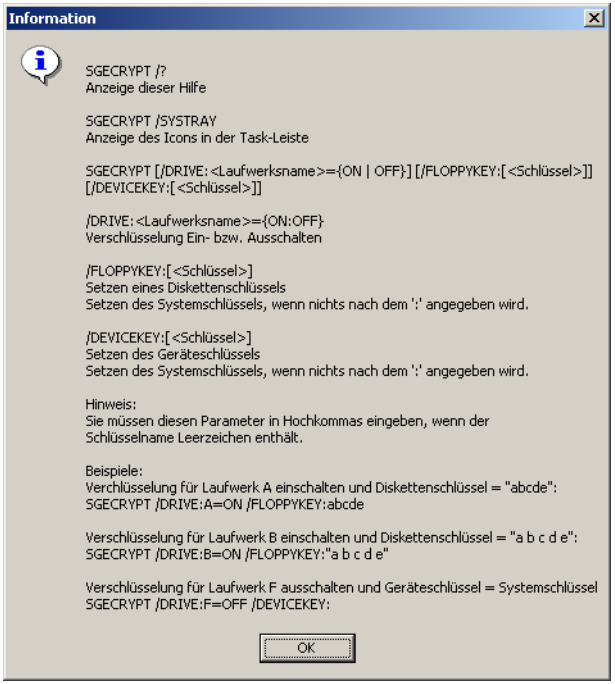
Ist der Haken vor der Option „Rücksetzen der Verschlüsselungseinstellungen beim Abmelden“ entfernt, werden die temporären Schlüssel nicht mehr zurückgesetzt.



21.4 Verschlüsselungseinstellungen über Kommandozeile schalten

Die Disketten-/Geräteverschlüsselung kann auch von der Kommandozeile aus gestartet werden.

Die mögliche Kommandozeilensyntax zeigt der Befehl `SGECRYPT /?` an.


Information
SGECRYPT /?
Anzeige dieser Hilfe
SGECRYPT /SYSTRAY
Anzeige des Icons in der Task-Leiste
SGECRYPT [/DRIVE:<Laufwerksname>={ON | OFF}] [/FLOPPYKEY:[<Schlüssel>]] [/DEVICEKEY:[<Schlüssel>]]
/DRIVE:<Laufwerksname>={ON:OFF}
Verschlüsselung Ein- bzw. Ausschalten
/FLOPPYKEY:[<Schlüssel>]
Setzen eines Diskettenschlüssels
Setzen des Systemschlüssels, wenn nichts nach dem ':' angegeben wird.
/DEVICEKEY:[<Schlüssel>]
Setzen des Geräteschlüssels
Setzen des Systemschlüssels, wenn nichts nach dem ':' angegeben wird.
Hinweis:
Sie müssen diesen Parameter in Hochkommas eingeben, wenn der Schlüsselname Leerzeichen enthält.
Beispiele:
Verchlüsselung für Laufwerk A einschalten und Diskettenschlüssel = "abcde":
SGECRYPT /DRIVE:A=ON /FLOPPYKEY:abcde
Verschlüsselung für Laufwerk B einschalten und Diskettenschlüssel = "a b c d e":
SGECRYPT /DRIVE:B=ON /FLOPPYKEY:"a b c d e"
Verschlüsselung für Laufwerk F ausschalten und Geräteschlüssel = Systemschlüssel
SGECRYPT /DRIVE:F=OFF /DEVICEKEY:
OK

21.5 Hinweise zur Disketten- und Geräteverschlüsselung

- **Schlüssel und Algorithmus**
  Verschlüsselt wird ein Datenträger sowohl mit Schlüssel als auch mit Algorithmus. Informieren Sie sich bitte, welche Algorithmen für Disketten- und/oder Wechselmedienlaufwerke auf der jeweiligen Arbeitsstation verwendet werden.

BEISPIEL:
Disketten einer Arbeitsstation werden mit dem DES-Algorithmus verschlüsselt. Sie speichern wichtige Daten auf einer Diskette ab, um Sie an einem anderen Rechner wieder einzulesen. Werden dort Disketten mit IDEA verschlüsselt, wird der Zugriff auf die Daten verweigert.

- **Lesen verschlüsselter Medien**
  Vorsichtig muss auch verfahren werden, wenn Sie versuchen verschlüsselte Datenträger in einem unverschlüsselten Laufwerk zu lesen und umgekehrt. Legt man in ein unverschlüsseltes Laufwerk ein verschlüsseltes Wechselmedium ein, erhalten Sie vom Betriebssystem die Meldung, dass das Dateisystem Ihres (verschlüsselten) Mediums ungültig ist. Würden Sie dieses nun aufgrund dieser Meldung in dem unverschlüsselten Laufwerk formatieren, sind die dort gespeicherten Daten unwiederbringlich verloren.

- **Verschlüsselung ein-/ausschalten**
  Das Ein-/Ausschalten der Verschlüsselung von Disketten bzw. Wechselmedien in der SafeGuard Easy-Administration ist sofort wirksam, während die Neuvergabe von Rechten für SGECRYPT erst nach einem Neustart gültig wird.

- **Warnmeldung**
  Beim Zugriff auf unformatierte oder verschlüsselte Disketten/Wechselmedien erscheint eine Meldung, die vor dem Verlust von Daten bei einer Formatierung warnt.

22 FIPS 140-2 (Level 1) Zertifizierung

Die FIPS-Zertifizierung beschreibt Sicherheitsanforderungen für Verschlüsselungsmodule. Beispielsweise verlangen Regierungsbehörden in den USA und in Kanada FIPS 140-2-zertifizierte Software für besonders sicherheitskritische Informationen.

Kennzeichen einer FIPS-konformen SafeGuard Easy-Installation ist, dass nur bestimmte Algorithmen für die Verschlüsselung verwendet werden dürfen, und zwar:

- AES-128
- AES-256
- 3DES

Wenn SafeGuard Easy im FIPS-Modus installiert ist, erscheint ein Icon in der Taskleiste.

22.1 Neue Funktionen für FIPS

Um die Anforderungen für die FIPS 140-2 Zertifizierung zu erfüllen, unterstützt SafeGuard Easy diese beiden neuen Funktionalitäten:

Known Answer Test (KAT)
Der Known Answer Test wird durchgeführt, um zu testen, ob die eingesetzten Krypto-Algorithmen korrekt arbeiten und korrekte Ergebnisse liefern. Der KAT wird für alle von FIPS zugelassenen Krypto-Algorithmen ausgeführt, auch für die Hashfunktion HMAC-256, die beim Integritätscheck verwendet wird.

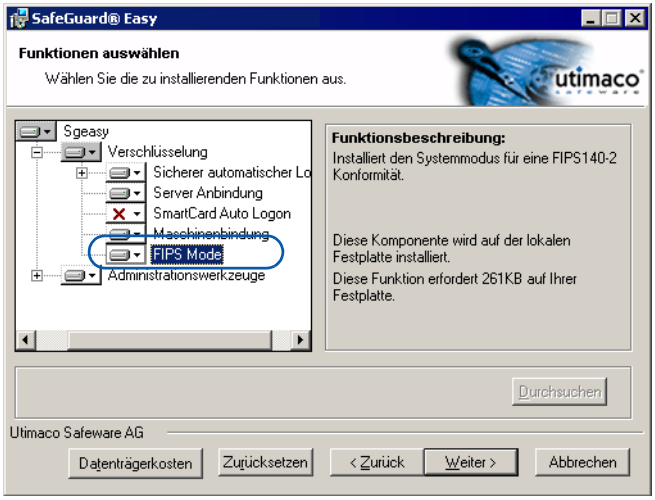
Für den KAT verschlüsselt ein Verschlüsselungsmodul einen definierten Datenblock und überprüft das Verschlüsselungsresultat, wenn die erzeugten verschlüsselten Daten die erwarteten Daten sind. Wenn das Resultat falsch ist, muss das Verschlüsselungsmodul jeden weiteren Verschlüsselungsprozess sperren. Verschlüsselungstreiber von SafeGuard Easy führen einen Known Answer Test (KAT) automatisch nach der Initialisierung des Treibers durch. Der KAT wird für Verschlüsselung und Dekodierung durchgeführt. Die installierten Verschlüsselungsmodule innerhalb des SafeGuard Easy-Systemkerns führen die gleichen Tests durch.

Integritätscheck
Ein Integritätscheck wird für die Verschlüsselungsmodule durchgeführt, um sicherzustellen, dass die Module nicht geändert wurden. Wenn ein Integritätscheck fehlschlägt, stoppt das System alle weiteren Prozesse. Dieser Test wird durchgeführt für die Verschlüsselungstreiberdateien von SafeGuard Easy und die Verschlüsselungsmodule innerhalb des SafeGuard Easy Systemkerns. Zusätzlich wird der Integritätscheck für die Systemdaten innerhalb des Systemkerns durchgeführt, um illegale Manipulationen zu entdecken.

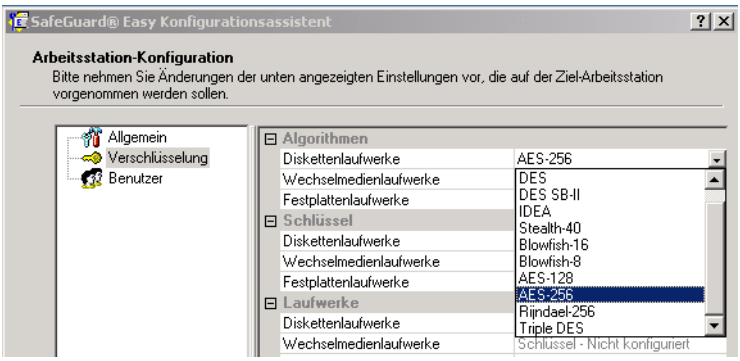
Sobald SafeGuard Easy FIPS-konform installiert wird, werden beide Testverfahren für den Systemkern und den Win32-Modus ausgeführt. Der KAT sogar auch, wenn der FIPS-Modus nicht aktiv ist.

22.2 SafeGuard Easy FIPS-konform installieren

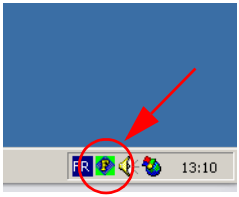
Eine Einstellung während der Installation („FIPS-Modus“) legt fest, ob ein SafeGuard Easy-System FIPS-konform sein soll.



Im weiteren Verlauf der Installation muss für die verschiedenen Laufwerke jeweils einer der geforderten Algorithmen ausgewählt werden (AES-128, AES-256, 3DES).



Nach Abschluss der Installation zeigt ein Icon in der Systemleiste an, dass SafeGuard Easy im FIPS-Modus läuft.



Wenn im Verlauf der Installation andere Algorithmen als die zugelassenen ausgewählt werden, löst SafeGuard Easy eine Fehlermeldung aus.

SafeGuard Easy bricht nach Bestätigen der Fehlermeldung die Installation ab, und der Benutzer muss den Installationsvorgang erneut starten.

22.3 Sicherer Einsatz von SafeGuard Easy in zertifizierter Konfiguration

Um SafeGuard Easy in einer zertifizierte Konfiguration einzusetzen und damit die mit dem Produkt gelieferte höchstmögliche Sicherheit zu gewährleisten, sollte das System folgendermaßen konfiguriert sein:

- Installation mit Pre-Boot Authentisierung
- Minimale Passwortlänge: 6 Zeichen
- Algorithmen AES-128, AES-256 oder 3DES verwenden.
- Vollständige Verschlüsselung der Festplatte aktivieren
- Disketten-/Wechselmedienverschlüsselung aktivieren
- Benutzer dürfen Disketten-/Wechselmedienverschlüsselung nicht schalten
- SafeGuard Easy Bildschirmsperre aktivieren
- Bei der manuellen Definition von Schlüsseln ist eine möglichst große Anzahl von zufällig gewählten Zeichen (max. 32 Zeichen) einzugeben. Es sollten keine trivialen Schlüssel vergeben werden, da diese leicht von einem Angreifer erraten werden können.

23 SafeGuard Easy und Lenovo Thinkvantage Technologien - Embedded Security Subsystem (ESS Chip)

Die Trusted Computing Group (TCG) hat sich als Zusammenschluss internationaler Hersteller zum Ziel gesetzt, die Sicherheit und Vertrauenswürdigkeit moderner Computer Plattformen und Betriebssysteme zu verbessern.

Als Kerntechnologie dient das Trusted Platform Module (TPM), ein in das Motherboard eingebauter kryptographischer Hardware-Chip, welcher als kryptografisches Device, als sicherer Schlüsselspeicher und Zufallszahlengenerator dient.

Ähnlich wie bei Smartcards benötigt auch das TPM passende Software um seine Leistungsfähigkeit entfalten zu können. In seinen Basisfunktionen kann das TPM Schlüssel gesichert verwalten und diese über Standardmechanismen wie Cryptographic Service Provider (CSP) für Benutzer und Applikationen nutzbar machen, verschlüsselt jedoch selbst keine Betriebssystem- oder Nutzerdaten. Darüber hinaus können durch die Nutzung des TPM neue Sicherheitskonzepte, wie etwa Maschinenbindung, realisiert werden.

Lenovo rüstet bereits heute eine Vielzahl seiner Notebooks und Desktop PCs mit einem TCG konformen Sicherheits-Chip aus. Lenovo nennt das System ESS (Embedded Security Subsystem) und die zugehörige Client Software „Client Security Software“ (CSS). Lenovo ist seit langem der führende Anbieter von Notebooks mit TPM und war bis vor kurzem der einzige Anbieter am Markt mit einer etablierten Lösung.

Utimaco Safeware ergänzt nun als erster professioneller Anbieter die Lenovo Basislösung um eine ESS-fähige Festplattenverschlüsselung und weitere Sicherheitsprodukte. Diese zeigen, wie Anwender bestmögliche Vorteile aus „Sicherheit in Hardware“ bei gleichzeitiger voller Kontrolle über Ihre Infrastruktur ziehen können.

Für weiterführende Informationen zu TPM, ESS und CSS schlagen Sie bitte in Ihrer Lenovo Dokumentation nach.

23.1 SafeGuard Easy und TPM

Die SafeGuard Easy TPM Unterstützung bietet eine erweiterte Funktionalität für PCs mit ESS/TPM Chip. Die wichtigsten Funktionen sind:

- **Client Security Integration**
  Wenn Benutzer von Arbeitsstationen mit TPM-Chip die CSS (Client Security Solution) weiterhin verwenden wollen, bindet SafeGuard Easy diese Funktion problemlos ein.
  Wird SafeGuard Easy mit CSS kombiniert, besteht für den Benutzer die Möglichkeit, sich nach der Pre-Boot Authentisierung automatisch an das TPM anmelden zu lassen. Die Daten werden in diesem Fall von SafeGuard Easy gespeichert, automatisch an den SafeGuard Logon Prozess weitergegeben, und der Benutzer wird nicht durch zusätzliche Passwörter belastet.

- **Zufallsschlüssel über TPM erzeugen**
  Der ESS/TPM Chip besitzt einen Generator, der Zufallszahlen erzeugt. SafeGuard Easy nutzt diesen Mechanismus zum Erzeugen von Session Keys und Zufallsschlüsseln.

- **Verbindung von SafeGuard Easy Client und SafeGuard Easy Server über TPM sichern**
  SafeGuard Easy kann den TPM-Generator auch für die Sicherung der Verbindung Client-Server im Rahmen der zentralen Administration nutzen.
  SafeGuard Easy Client und SafeGuard Easy Server erzeugen im Rahmen der zentralen Administration jeweils ein RSA-Schlüsselpaar, um sich gegenseitig zu authentisieren und die Verbindung zur Datenbank abzusichern. Dieses Schlüsselpaar kann auch vom ESS/TPM Chip erzeugt werden.

- **Maschinenbindung**
  Ermöglicht die Bindung einer Festplatte an ein bestimmtes ESS/TPM. Es ist dann nicht mehr möglich, eine eventuell gestohlene Festplatte in einem anderen Computer zu verwenden. Auch dann nicht, wenn das Passwort bekannt ist.

23.2 Chip-Nutzung vorbereiten

Bevor der Chip genutzt werden kann (und **vor der Installation von SafeGuard Easy**), sind folgende Vorbereitungen zu treffen:

1. Sicherstellen, dass der ESS Chip im BIOS aktiviert ist.
2. Atmel Treiber für den ESS/TPM Chip installieren.

   Ab CSS 6.0 nicht mehr erforderlich!
3. SMBus Treiber installieren (jedes Lenovo Thinkpad hat einen eigenen Treiber).
4. Für SafeGuard Easy benötigen Sie folgende Versionen der „Client Security Software“ (CSS).
   - **Für die Erzeugung von Zufallsschlüsseln und Client Security Integration:**
     „Client Security Software“ (CSS) Version 5.21. und höher
   - **Für die Client/Server Authentisierung:**
     „Client Security Software“ (CSS) Version 5.30. und höher

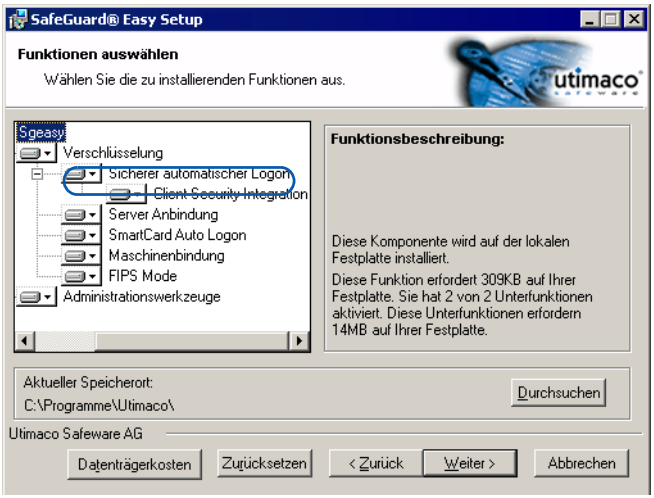
23.3 Erforderliche Einstellungen für Client Security Integration

Die CSS Integration von SafeGuard Easy setzt einen entsprechend konfiguriertes CSS voraus. Details lesen Sie bitte im Handbuch zu CSS nach.

So kombinieren Sie CSS und SafeGuard Easy:

1. Chip-Nutzung vorbereiten.
2. Beim Konfigurieren der Client Security Software ist darauf zu achten, dass „Ersetzen der normalen Windows-Anmeldung durch die gesicherte Anmeldung des Lenovo Security Clients“ aktiviert wird!

   Ab CSS 6.0 nicht mehr erforderlich.
3. SafeGuard Easy installieren.
   Bei der SafeGuard Easy Installation ist darauf zu achten, dass die Option „Client Security Integration“ aktiviert wird.



Ansonsten müssen Sie in SafeGuard Easy keine weiteren speziellen Konfigurationseinstellungen vornehmen.

4. Nach dem Neustart erhalten Sie einen veränderten Anmeldebildschirm, der statt dem regulären Windows-Passwort die „Passphrase“ verlangt.

CSS Integration und die sichere automatische Logon (SAL) Funktion von SafeGuard Easy

Der SAL legt die Windows-Daten nach einmaliger Eingabe in einem geschützten Bereich ab und greift nach jeder erfolgreichen Benutzer-Anmeldung in der Pre-Boot Authentisierung darauf zurück, um den Benutzer automatisiert am Betriebssystem anzumelden (siehe ’Windows-Anmeldung konfigurieren’).

Ähnlich verhält es sich, wenn CSS Integration und SAL zusammen auf einem PC eingesetzt werden: Die Passphrase wird verschlüsselt abgelegt und muss nicht mehr eingegeben werden. Anmeldedaten werden nur in der Pre-Boot Authentisierung abgefragt.

HINWEIS:
Wenn SAL für die normale Windows-Anmeldung aktiviert war, muss vor der CSS Integration die Datei `SGSAL.dat` (zu finden unter <Systemlaufwerk>`/System32`) gelöscht werden.
`SGSAL.dat` muss neu angelegt werden, weil sich die TPM-Daten im Format von denen einer normalen Windows-Anmeldung unterscheiden. Daher darf keine `SGSAL.dat` existieren, wenn CSS/SAL funktionieren soll.

23.4 Erforderliche Einstellungen für die Erzeugung von Zufallsschlüsseln über den TPM Chip

Die Erzeugung von Zufallsschlüsseln über den ESS/TPM-Chip erzwingen Registrierungseinträge, die **vor der Installation von SafeGuard Easy** angelegt werden müssen.

So erzeugen Sie Zufallsschlüssel mit dem TPM Chip:

1. Chip-Nutzung vorbereiten (siehe 'Chip-Nutzung vorbereiten').
2. In der Windows-Registrierung unter
   HKEY_LOCAL_MACHINE
   SOFTWARE
   Utimaco
   SGEasy

   folgende Einträge anlegen:

   Cryptographic Service Provider [Zeichenfolge]
   Als Wert muss eingetragen werden:
   a) für CSS<= 5.40:
   „IBM Embedded Security Subsystem Enhanced CSP"
   b) für CSS>= 6.0
   „ThinkVantage Client Security Solution CSP"

   UseCSPRandomGenerator [DWORD-Wert]
   Der Wert muss auf „1" gesetzt werden.
3. SafeGuard Easy installieren.

Die Zufallsschlüssel werden nun ohne weitere Konfigurationseinstellungen vom ESS/TPM Chip erzeugt.

23.5 Erforderliche Einstellungen für die Sicherung der Client-/ Server-Authentisierung über den TPM Chip

Einstellungen für Client Security Software (CSS) <= 5.40

Das Erzeugen von Schlüsselpaaren über den ESS/TPM Chip ist bis CSS 5.40 über das Administrator-Passwort des Chips abgesichert. Das Administrator-Passwort wird während der Installation der CSS Software festgelegt. Wird SafeGuard Easy im Rahmen einer zentralen Installation auf Clients mit TPM Chip verteilt, wird das Administrator-Passwort in einem Dialog abgefragt. In Netzwerken mit mehreren TPM-Clients kennen reguläre Benutzer in der Regel aber das Administrator-Passwort des Chips nicht, und oft möchten Administratoren für alle TPM Rechner im Netz ein identisches Administrator-Passwort verwenden.

Ein SafeGuard Easy-Tool erzeugt zu diesem Zweck eine verschlüsselte Datei mit dem Administrator-Passwort für den Chip. Diese Datei wird im Rahmen einer zentralen Installation an die TPM-Clients verteilt.

SafeGuard Easy befüllt dann auf Client-Seite automatisch den Dialog, der das Administrator-Passwort abfragt und ermöglicht so die RSA-Schlüsselgenerierung ohne Benutzerinteraktion.

So erzeugen Sie RSA Schlüsselpaare mit dem TPM Chip:

1. Chip-Nutzung auf Client/Server vorbereiten (siehe 'Chip-Nutzung vorbereiten').
2. In der Windows-Registrierung des Clients/Servers unter

   HKEY_LOCAL_MACHINE
   SOFTWARE
   Utimaco
   SGEasy

   folgende Einträge anlegen:

   Cryptographic Service Provider [Zeichenfolge]
   Als Wert muss eingetragen werden:
   „IBM Embedded Security Subsystem Enhanced CSP"

   ForceCSPUsage [DWORD-Wert]
   Der Wert muss auf „1" gesetzt werden.
   (ForceCSPUsage übernimmt auch die Erzeugung von Zufallsschlüsseln.)
3. Auf einem PC mit installiertem SafeGuard Easy das Tool `SGTpmApn.exe` aufrufen und die verschlüsselte Datei mit dem Administrator-Passwort für den ESS/TPM Chip erstellen. Wenn der Standardname dieser Datei umbenannt wird, in der Windows-Registrierung des Clients unter

   HKEY_LOCAL_MACHINE
   SOFTWARE
   Utimaco
   SGEasy
   folgenden Eintrag angelegen:

   ESSAdminPassword [Zeichenfolge]

Als Wert muss die Datei mit dem Administrator-Passwort eingetragen werden, z.B.:
`D:\Programme\Utimaco\SafeGuard Easy\AdminPW.dat`

4. Verschlüsselte Datei zusammen mit den SafeGuard Easy-Paketen an die Clients verteilen. Die Datei mit dem Administrator-Passwort muss im SafeGuard Easy Installationsverzeichnis liegen.

Unmittelbar vor der RSA Schlüsselgenerierung startet SafeGuard Easy einen Monitor, der das Administrator-Passwort aus der Datei liest, den Passwort Dialog des ESS CSP automatisch befüllt und die Datei anschließend löscht.

Nach der Installation von SafeGuard Easy wird das RSA Schlüsselpaar automatisch erzeugt, und der Benutzer muss keine weiteren Konfigurationseinstellungen durchführen.

Einstellungen für Client Security Software (CSS) >= 6.0

Ab CSS Version 6.0 wird das Administrator-Passwort bei einer interaktiven RSA-Schlüsselgenerierung nicht mehr abgefragt, d.h. es muss keine mit dem SafeGuard Easy-Tool verschlüsselte Datei erstellt und verteilt werden wie bei CSS <= 5.40.

So erzeugen Sie RSA-Schlüsselpaare mit dem TPM-Chip:

1. In der Windows-Registrierung des Clients/Servers unter

   HKEY_LOCAL_MACHINE
   SOFTWARE
   Utimaco
   SGEasy

   folgende Einträge anlegen:

   Cryptographic Service Provider [Zeichenfolge]
   Als Wert muss eingetragen werden:
   „ThinkVantage Client Security Solution CSP“

ForceCSPUsage [DWORD-Wert]
Der Wert muss auf „1“ gesetzt werden.
(ForceCSPUsage übernimmt auch die Erzeugung von Zufallsschlüsseln.)

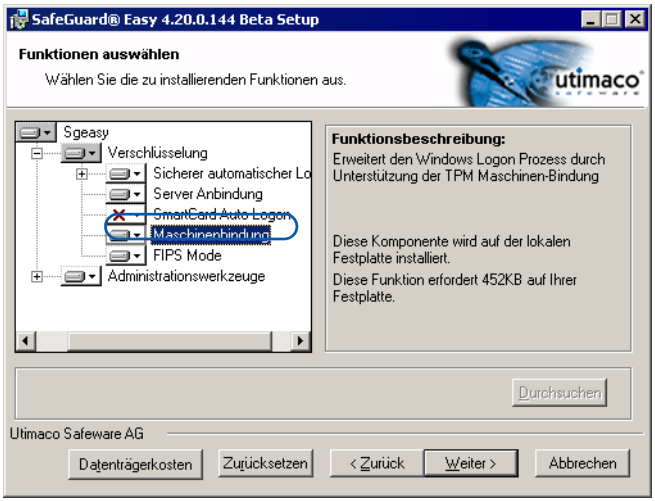
HINWEIS:
Die Erzeugung der Schlüsselpaare über den TPM-Chip ist deutlich langsamer als die reine Software-Lösung, was zu Performance-Einbußen führen kann. Die Performance-Einbußen werden durch den Authentisierungsvorgang von Client und Server verursacht, nicht durch Verschlüsselungsvorgänge.

23.6 Erforderliche Einstellungen für die Maschinenbindung

Die Maschinenbindung erzeugt eine eindeutige Verbindung zwischen dem Computer und der angeschlossenen Festplatte. Dies erfolgt über eine Signatur, die auf Übereinstimmung mit jener Signatur, die beim Ausführen der initialen Maschinenbindung erzeugt wurde, geprüft wird.
Die Referenzsignatur wird in der Registrierung gespeichert. Der Boot-Prozess wird nur fortgesetzt, wenn die Signaturen identisch sind. In jedem anderen Fall wird der Boot-Prozess abgebrochen.

So kombinieren Sie die Maschinenbindung und SafeGuard Easy:

1. Chip-Nutzung vorbereiten.
2. SafeGuard Easy installieren.
   Bei der SafeGuard Easy Installation ist darauf zu achten, dass die Option „Maschinenbindung“ aktiviert wird.



23.6.1 Initiale Maschinenbindung

Beim ersten Hochfahren des Computers nach der Installation der Maschinenbindung, wird der SafeGuard Assistent für die Maschinenbindung gestartet. Sie informiert, dass die Maschinenbindung für diesen Computer noch nicht aktiviert wurde.

SafeGuard Authentication - Maschinenbindung
[SafeGuard® Authentication]
utimaco
Wilkommen zum Assistenten der Maschinenbindung!
SafeGuard Authentication sorgt für eine sichere Anmeldung auf Ihren Computer und schützt vor Verwendung der Festplatte in einem anderen Computer oder Laptop.
Die Maschinenbindung dieses Computers ist noch nicht aktiviert. Um sie zu aktivieren, geben Sie bitte die Administratorpassphrase des Sicherheitschips ein. Nach Bestätigung der Passphrase wird für Ihren Computer ein eindeutiger Geheimschlüssel generiert.
Drücken Sie auf Fortsetzen um der Prozess fortzusetzen oder auf Herunterfahren um den Computer herunterzufahren.
Fortsetzen >>
Herunterfahren

HINWEIS:
CSS < 6.0: Security Chip Passwort erforderlich.
CSS >= 6.0: Kein Security Chip Passwort erforderlich.

Klicken Sie auf **Fortsetzen**, um den Prozess der initialen Maschinenbindung zu starten.

Da jede Operation auf dem Security Chip, die den privaten Schlüssel betrifft, ein Passwort erfordert, muss das Security Chip Passwort eingegeben werden
CSS 6.0 verlangt kein Security Chip Passwort.

Enter Administrator Password
Before you can complete an IP Security certificate request, you must enter the IBM Security Chip password below.
Too many consecutive incorrect entries will cause the security subsystem to be locked for increasing periods of time.
OK
Exit

Ein Dialog bestätigt die erfolgreiche Maschinenbindung. Die lokale Festplatte kann nun ausschließlich mit diesem Computer verwendet werden.

SafeGuard Authentication - Maschinenbindung beendet
[SafeGuard® Authentication]
utimaco
Der Prozess zur Maschinenbindung wurde erfolgreich abgeschlossen.
Die SafeGuard Authentication Software kontrolliert jetzt die Hardware Ihres Computers. Die lokale Festplatte kann nur noch zum Hochfahren dieses Computers verwendet werden.
Für Informationen zur Herstellung einer Sicherungskopie, schlagen Sie bitte im Handbuch nach.
Schließen

Bei jedem folgenden Hochfahren des Computers prüft die Software den Status der Maschinenbindung. Der Bootvorgang wird nur fortgesetzt, wenn die Signaturen identisch sind.

23.6.2 Maschinenbindung gescheitert

SafeGuard Authentication - Maschinenbindung gescheitert
[SafeGuard® Authentication]
utimaco
Die Überprüfung der Maschinenbindung ist gescheitert!
Es könnte sein, dass die lokale Festplatte an einem anderen Computer angemeldet ist, oder dass die Einstellung der Sichersheit-Hardware geändert wurde beziehungsweise korrumpiert wurde.
Für zusätzliche Hilfe, setzen Sie sich bitte mit Ihrem Sicherheitsadministrator in Verbindung.
Herunterfahren
Wiederherstellen

Folgende Situationen verursachen ein Scheitern der Verifikation der Signaturen:

- Das Hardware Sicherheitsmodul ist deaktiviert.
- Das Hardware Sicherheitsmodul ist beschädigt.
- Der Master Key des Sicherheitsmoduls wurde geändert.
- Die Referenzsignatur wurde verändert.
- Die Referenzsignatur fehlt.
- Das für die Signieroperation verwendete Schlüsselpaar wurde verändert.
- Der verwendete CSP funktioniert nicht oder wurde geändert.
- Die CSS Konfiguration wurde geändert.

Um trotz gescheiterter Maschinenbindung den Zugang zum System zu ermöglichen, wird in diesem Dialog eine Wiederherstellungsfunktion angeboten.

Für das Wiederherstellen des Systems über ein Backup des Embedded Security System (ESS) schlagen Sie bitte in Ihrer Lenovo Dokumentation nach.

23.6.3 Maschinenbindung Wiederherstellung

Damit Sie bei einer gescheiterten Maschinenbindung wieder Zugang zum System erlangen, klicken Sie auf die Schaltfläche **Wiederherstellen**
.

In diesem Dialog muss jenes Security Chip Passwort angegeben werden, das bei der initialen Maschinenbindung angegeben wurde. Auch dann, wenn das Passwort nach der initialen Maschinenbindung geändert wurde. Wird die Wiederherstellungsfunktion verwendet, weil ein neuer Security Chip eingebaut wurde, muss zur Wiederherstellung das Passwort des alten Chips eingegeben werden.

Ab CSS >= 6.0 wird der Dialog durch den Standard-„SafeGuard Authentication - Wiederherstellung“ Dialog ersetzt und Windows-Benutzer, Passwort und Domäne abgefragt.

Nachdem Sie wieder Zugang zum System haben, müssen Sie die initiale Maschinenbindung erneut ausführen, wenn eine der folgenden Situationen das Scheitern der Verifikation verursacht hat:

- Das Hardware Sicherheitsmodul ist beschädigt.
- Der Master Key des Sicherheitsmoduls wurde geändert.
- Die Referenzsignatur wurde verändert.
- Die Referenzsignatur fehlt.
- Das für die Signieroperation verwendete Schlüsselpaar wurde verändert.

Bevor die Maschinenbindung erneut ausgeführt wird, müssen Sie

1. unbedingt folgende Werte in der Registrierung löschen:
   - **Machine Binding**
   - **Recovery**

   unter dem Schlüssel:

   HKEY_LOCAL_MACHINE
   SOFTWARE
   Utimaco
   SGLogon
   Embedded Security System

> ***ACHTUNG:***
> Diese Werte müssen unbedingt gelöscht werden, bevor Sie die Maschinenbindung erneut ausführen. Sind diese Werte beim Ausführen einer erneuten Maschinenbindung vorhanden, kann es zu einer Situation kommen, in der Sie keinen Zugang zum System mehr haben.

2. Müssen die auf dem Security Chip vorhandenen Daten mit Hilfe von Lenovo Tools zurückgesetzt werden.

Die erneute initiale Maschinenbindung startet automatisch beim nächsten Starten des Systems.

23.6.4 Konfiguration des Wiederherstellungsmodus

Neben dem Standarddialog zur Wiederherstellung des Systems, bietet die SafeGuard Authentication TPM Unterstützung einen zweiten Dialog zur Autorisierung der Wiederherstellung an. In diesem Dialog wird der Benutzername, Passwort und optional der Domänenname eines Benutzers mit Administratorrechten verwendet, um wieder Zugriff auf das System zu erlangen.

Welcher Dialog verwendet wird, kann über die administrative Vorlage, die bei der Verwendung der TPM-Unterstützung installiert wird, eingestellt werden.

Sie finden die Einstellung in der Management Konsole unter:

Computerkonfiguration
\Administrative Vorlagen
\SafeGuard
\Authentication
\Machine Binding
\Wiederherstellung

Unter *Wiederherstellungsart* kann

- **Administrative Zugangsdaten**
  für die Verwendung des Windows Benutzernamens und des Passworts bzw.
- **TPM Passwort (Standardeinstellung)**
  für die Verwendung des Security Chip Passworts

ausgewählt werden.

Geben Sie im angezeigten Dialog Benutzernamen und Passwort eines auf dem Rechner existierenden Benutzers ein. Der Domänenname ist optional.

HINWEIS:
Der Benutzer muss auf diesem Rechner Administratorrechte besitzen.

24 SafeGuard Easy und Lenovo Thinkvantage Technologien - Rescue and Recovery™

SafeGuard Easy ist kompatibel mit Rescue and Recovery™. Das erlaubt Benutzern, Lenovos effiziente Backup- und Restore-Methode zu nutzen, auch wenn die Betriebssystem-Partition mit SafeGuard Easy verschlüsselt ist. SafeGuard Easy bietet hier eine einzigartige Funktionalität unter Produkten zur Festplattenverschlüsselung.

24.1 Überblick

Rescue and Recovery™ bietet als zentrale Funktion die Wiederherstellung von Daten per Tastendruck. Auch wenn das primäre Betriebssystem beschädigt ist und nicht mehr bootet, rettet Rescue and Recovery™ Daten über eine Notfall-Umgebung. Die Rettungs-Tools sind aufrufbar über den Microsoft Windows Desktop oder die in Lenovo-Systeme integrierte, blaue „Thinkvantage“ (ehem. „Access IBM“) -Taste. Rescue and Recovery™ unterstützt aber auch Nicht-Lenovo-Systeme. Rescue and Recovery™ zielt primär auf mobile Endbenutzer, die maximale Sicherheit für ihre Notebooks anstreben, aber sich im Fall eines Systemproblems selbst helfen müssen.

Utimaco Safeware ergänzt als erster professioneller Anbieter von Festplattenverschlüsselung die Lenovo-Lösung um die Möglichkeit, beschädigte Systeme wiederherzustellen, ohne die Verschlüsselung zu verlieren. Verfügbarkeit, Integrität und Vertraulichkeit von Daten ist mit der Kombination von Rescue and Recovery und SafeGuard Easy garantiert.

Für weiterführende Informationen zu Rescue and Recovery™ schlagen Sie bitte in Ihrer Lenovo Dokumentation nach.

24.2 Rescue and Recovery und SafeGuard Easy

SafeGuard Easy integriert sich reibungslos in die Rescue and Recovery-Vorgaben und unterstützt natürlich auch Lenovo-eigene Features wie den „Thinkvantage“ (ehem. Access IBM) Button auf der Tastatur von Notebooks oder den blauen „Eingabe“ Button bei Desktop-PCs.

Angenommen ein Benutzer verschlüsselt die komplette Festplatte mit SafeGuard Easy, wird er unmittelbar nach der Installation aufgefordert, eine Sicherungskopie zu erstellen. In diesem Systemabbild enthalten sind u.a. die SafeGuard Easy Treiber, so dass nach dem Restore dieses Systemabbilds Windows weiterhin fehlerfrei verschlüsselt bootet (Die Sicherungskopie mit SafeGuard Easy und seinen Treibern wird im folgenden kurz „SafeGuard Easy-Backup“ genannt).

Gibt es einen System-Crash, stellt der Benutzer über die Notfall-Umgebung von Rescue and Recovery™ den gespeicherten SafeGuard Easy-Backup wieder her. Vor dem Wiederherstellen werden die SafeGuard Easy-Benutzerdaten in der Pre-Boot Authentisierung abgefragt, Festplattenschlüssel und Algorithmus sind also vorhanden.

SafeGuard Easy „überlebt“ einen System-Restore, ohne dabei die Verschlüsselung zu verlieren und muss nicht neu installiert werden. Der Benutzer kann ohne Unterbrechung nach dem Restore weiterarbeiten und wird nicht durch erneutes Anstoßen der Verschlüsselung gestört.

24.2.1 Vorteile der Kombination Rescue and Recovery und SafeGuard Easy

- SafeGuard Easy verschlüsselt die komplette Festplatte inklusive temporärer Dateien, Auslagerungsdatei, Hibernation und Memory-Dump-Datei und schützt sie durch Abfrage der SafeGuard Easy-Zugangsdaten vor unerlaubtem Zugriff.
- Alle Sicherungskopien sind kryptographisch gesichert, sobald sie auf einer verschlüsselten lokalen Festplatte gespeichert sind.
- Rescue and Recovery stellt ein beschädigtes System schnell wieder her, ohne SafeGuard Easy neu installieren und die Festplatte erneut verschlüsseln zu müssen.
- Wiederherstellen eines SafeGuard Easy-Backups aus der Rescue and Recovery-Umgebung ist nur möglich, wenn vorher SafeGuard Easy-Zugangsdaten an der Pre-Boot Authentisierung eingetragen werden.

24.2.2 Voraussetzungen

- Lenovo-PC / Lenovo-Notebook
- aktuellstes BIOS für Ihr System
- SafeGuard Easy ab Version 4.10
- unterstützte Rescue and Recovery™-Versionen:
  - Rescue and Recovery™ 1.0 (Build 033)
  - Rescue and Recovery™ 2.0 (Build 2.00.0170)
  - Rescue and Recovery™ 3.0 (Build 3.00.0029.00)
  - Rescue and Recovery™ 4.0 (Build 4.0.0114)
  - Rescue and Recovery™ 4.2 (Build 4.20.0510)

24.3 Installation

In den folgenden Installationsbeispielen wird angenommen, dass die Rescue and Recovery-Umgebung nicht in die Service Partition installiert wird. Alle Besonderheiten, die bei einer Verwendung der Service Partition zu berücksichtigen sind, sind im Kapitel Besonderheiten' aufgelistet.

Wenn Sie Rescue and Recovery™ auf einer Festplatte ohne eine Service Partition installieren, wird Rescue and Recovery mit folgenden Standardeinstellungen für die Software installiert:

- Die Umgebung von Rescue and Recovery befindet sich standardmäßig auf einer virtuellen Partition, die auf Laufwerk C (primäre Partition des Master-Festplattenlaufwerks) des Computers installiert wird.
- Die virtuelle Partition besteht aus zwei Verzeichnissen, \minint und \preboot. Diese beiden Verzeichnisse werden durch Rescue and Recovery selbst geschützt.
- Die Sicherungen bzw. Sicherungskopien werden in der Standardeinstellung unter C:\RRUbackups gespeichert. Dieses Verzeichnis wird, wenn es sich auf der lokalen Partition des primären Festplattenlaufwerks befindet, durch Rescue and Recovery geschützt, damit es nicht gelöscht oder verschoben wird.

Bei der Installation von Rescue and Recovery™ und SafeGuard Easy ist die Installationsreihenfolge von Bedeutung. Bitte beachten Sie unbedingt die Anweisungen in den folgenden Kapiteln.

24.3.1 Weder SafeGuard Easy noch Rescue and Recovery™ sind installiert

1. Alle Rescue and Recovery mit Rapid Restore Versionen kleiner 4.0 deinstallieren!
2. Rescue and Recovery installieren.
3. SafeGuard Easy ab Version 4.10 installieren.

   SafeGuard Easy prüft, ob die richtige Version von Rescue and Recovery installiert ist und fügt seine Dateien und Einstellungen in die Lenovo Notfall-Umgebung ein.

   Bitte stellen Sie sicher, dass die Pre-Boot Authentisierung aktiviert ist, so dass kein Unbefugter unautorisiert beliebige Backups restaurieren kann.

   Die Pre-Boot Authentisierung wird während der Installation oder später in der Administration eingeschaltet über den Ordner Allgemein / Passworteinstellungen / Passwort beim Systemstart abfragen.

24.3.2 Nur SafeGuard Easy ist bereits installiert

SafeGuard Easy ab Version 4.10 ist installiert

1. Rescue and Recovery™ installieren.
2. Vor dem Reboot aus dem SafeGuard Easy-Verzeichnis nacheinander diese Tools aufrufen:
   - `MBRsync.exe`
   - `WinPERepair.exe`

SafeGuard Easy < 4.10 ist installiert

1. Auf SafeGuard Easy >= 4.10 updaten.
2. Rescue and Recovery™ installieren.
3. Vor dem Reboot aus dem SafeGuard Easy-Verzeichnis nacheinander diese Tools aufrufen:
   - `MBRsync.exe`
   - `WinPERepair.exe`

- oder -

1. Rescue and Recovery™ installieren
2. Vor dem Reboot aus dem SafeGuard Easy-Verzeichnis dieses Tool aufrufen:
   - `MBRsync.exe`
3. Auf SafeGuard Easy >= Version 4.10 updaten.

ACHTUNG:

Wann immer Rescue and Recovery™ nach SafeGuard Easy installiert wird, müssen vor dem Reboot, den Rescue and Recovery auslöst, die Tools „MBRsync.exe“ und „WinPErepair.exe“ ausgeführt werden. Beide Tools liegen im SafeGuard Easy-Verzeichnis und werden einfach per Doppelklick ausgeführt.

24.4 Upgrade

Upgrade bedeutet, dass sowohl SafeGuard Easy ab Version 4.10 und Rescue and Recovery™ installiert sind und eines der beiden Produkte aktualisiert wird.

24.4.1 Upgrade von SafeGuard Easy

Das Upgrade von SafeGuard Easy aktualisiert das komplette System inklusive Rescue and Recovery™. Es sind keine weiteren Aktionen nötig.

24.4.2 Upgrade von Rescue and Recovery

Wann immer Rescue and Recovery™ aktualisiert wird, müssen **vor dem Reboot** die Tools `MBRsync.exe` und `WinPErepair.exe` ausgeführt werden. Beide Tools liegen im SafeGuard Easy-Verzeichnis und werden einfach per Doppelklick aufgerufen.

24.5 Deinstallation

Bei der Deinstallation beider Produkte ist folgendes zu beachten:

- Deinstallieren Sie zunächst SafeGuard Easy und dann Rescue and Recovery.
- Die Deinstallation von SafeGuard Easy darf nicht unmittelbar auf einen System-Restore folgen. Starten Sie den PC neu und deinstallieren Sie danach SafeGuard Easy!

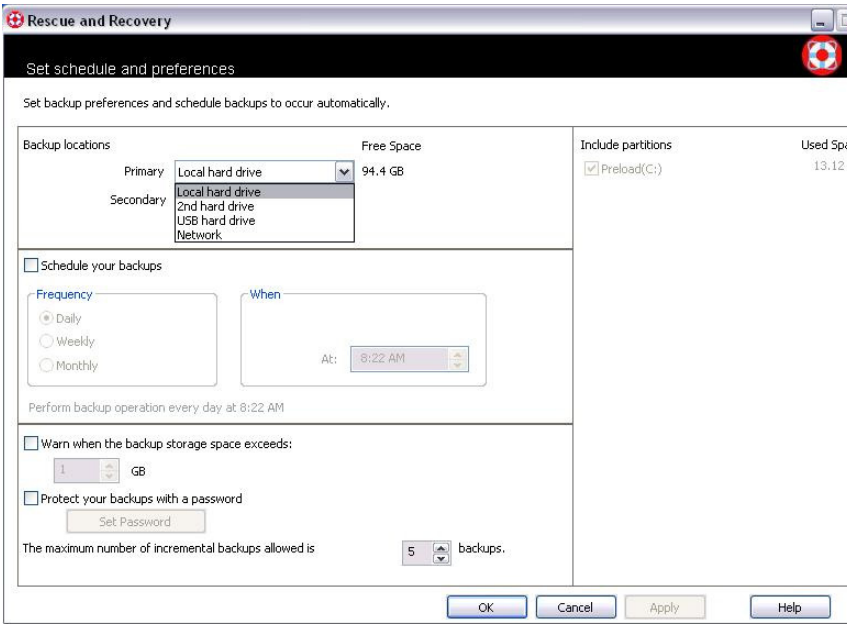
24.6 Sicherungskopie erstellen

Sicherungskopien werden über die Rescue and Recovery Software in der aktiven Windows-Umgebung erstellt. Auf PCs mit Rescue and Recovery rät SafeGuard Easy dem Benutzer nach einer erfolgreichen Installation unbedingt eine neue System-Sicherungskopie zu erstellen.

Wie Sie aus der Windows-Umgebung einen System-Backup erstellen, lesen Sie bitte in den entsprechenden Dokumenten von Lenovo nach.

SafeGuard Easy unterstützt für SafeGuard Easy-Backups folgende Medien:

- Lokale Festplatte
- 2. Festplattenlaufwerk
- USB-Festplattenlaufwerk
- Netzlaufwerk
- USB-Stick
- CD/DVD

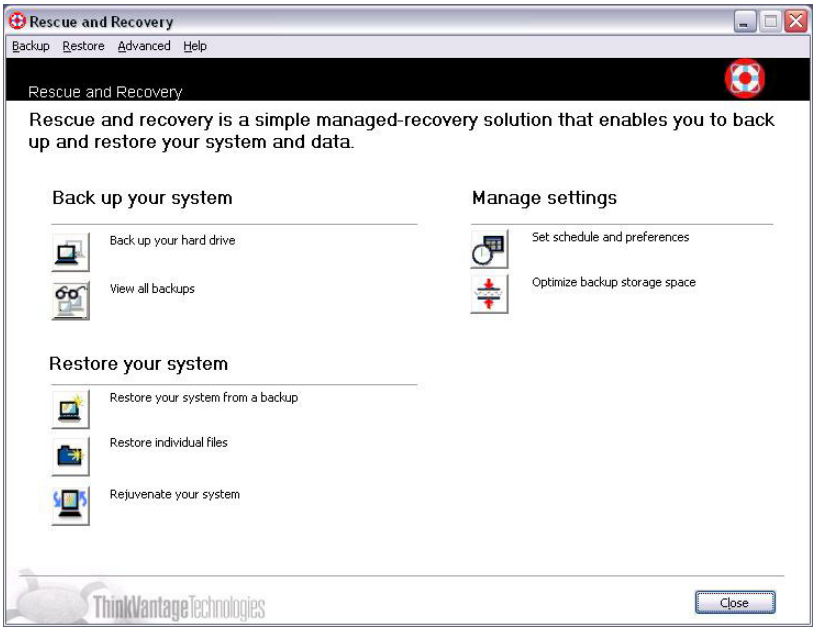


Die Sicherungen bzw. Sicherungskopien werden in der Standardeinstellung unter C:\RRUbackups gespeichert. Dieses Verzeichnis wird, wenn es sich auf der lokalen Partition des primären Festplattenlaufwerks befindet, durch Rescue and Recovery geschützt, damit es nicht gelöscht oder verschoben wird.

24.7 Dateien aus SafeGuard Easy-Backup wiederherstellen

Rescue and Recovery™ stellt einzelne Dateien oder Verzeichnisse aus einem Backup, der ein installiertes SafeGuard Easy enthält, problemlos wieder her.

Benutzer starten einfach Windows, dann die Rescue and Recovery Software und restaurieren die gesuchten Dateien. Es ist kein Neustart nötig, d.h. die restaurierten Daten stehen dem Benutzer sofort zur Weiterbearbeitung zur Verfügung.


Rescue and Recovery
Backup Restore Advanced Help
Rescue and Recovery
Rescue and recovery is a simple managed-recovery solution that enables you to back up and restore your system and data.
Back up your system
Back up your hard drive
View all backups
Manage settings
Set schedule and preferences
Optimize backup storage space
Restore your system
Restore your system from a backup
Restore individual files
Rejuvenate your system
ThinkVantage Technologies
Close

24.8 SafeGuard Easy-System wiederherstellen

Für den Restore eines System-Backups, der SafeGuard Easy enthält, startet der Benutzer die Rescue and Recovery-Umgebung. Diese erscheint, wenn beim Booten des PCs/Notebooks diese Tasten gedrückt werden:

- „Thinkvantage“/„Access IBM“ (bei Lenovo Notebooks).
- die „Blaue Eingabetaste“ (bei Lenovo Desktop-PCs).
- [F11] bei sonstigen Tastaturen.

Hinweis zu Rescue and Recovery™ 2.0:
Utimaco empfiehlt generell beim Restaurieren die komplette Festplatte wiederherzustellen. Wenn Sie jedoch versehentlich die Option „Nur das Windows-Betriebssystem und Applikationen aus einem Backup wiederherstellen“ gewählt haben, garantiert Utimaco nicht, dass die SafeGuard Easy-Dateien vollständig restauriert werden. Treten in diesem Fall Probleme beim Booten auf, müssen Sie jedoch keine negativen Folgen für ihr System befürchten. Rufen Sie nach einem Neustart einfach über die Lenovo-Tasten ihres PCs oder Notebooks die Rescue and Recovery™-Umgebung auf und stellen Sie die komplette Festplatte wieder her.

24.8.1 Boot-Umgebung

SafeGuard Easy erlaubt das Booten der Rescue and Recovery-Umgebung von...

- Lokaler Festplatte

  Virtuelle Partition auf der lokalen Festplatte oder lokale Service Partition

SafeGuard Easy erlaubt das Booten der Rescue and Recovery-Umgebung NICHT von...

- Bootfähiger CD
- Bootfähiger USB-Festplatte

Wird die Rescue and Recovery-Umgebung trotzdem von einem externen Medium gebootet, wird SafeGuard Easy während des Restore-Prozesses entfernt.

Um das System wieder abzusichern, muss SafeGuard Easy erneut installiert werden.

24.8.2 Vorgehensweise

1. Rescue and Recovery-Umgebung starten („Thinkvantage“-Taste, „Blauen Eingabetaste“ oder [F11]).
2. Die Pre-Boot Authentisierung erscheint und verlangt SafeGuard Easy-Zugangsdaten.
3. Die Benutzeroberfläche der Rescue and Recovery-Umgebung erscheint.
4. Den Willkommen-Bildschirm mit einem Klick auf Weiter beenden.
5. Im linken Menü **Über Sicherung wiederherstellen** wählen.
6. Der Dialog ***Von einer Sicherung wiederherstellen*** erscheint.
7. Den Backup, der ein installiertes SafeGuard Easy enthält, auswählen und wiederherstellen.

24.9 Service Partition und Factory Recovery Partition

Lenovo liefert neue PCs mit speziellen vorinstallierten Partitionen aus. Lenovo nennt diese Partitionen "Service Partion" und "Factory Recovery Partition":

- Service Partition: enthält die Rescue and Recovery-Bootumgebung.
- Factory Recovery Partition: enthält alle Informationen, um die Werkseinstellungen („Factory settings“) des Rechners wiederherzustellen.

Wenn auf Ihrem PC noch keine Service Partition vorhanden ist, Sie aber dennoch mit ihr arbeiten wollen, legen Sie sie vor der Installation von SafeGuard Easy an.

Wie Sie die Service Partition anlegen, schlagen Sie bitte in der entsprechenden Lenovo Dokumentation nach.

24.9.1 Besonderheiten

Folgende Besonderheiten sind bei Verwenden der Service Partition u nd der Factory Recovery Partition zu beachten:

Betriebs-system	**Verschlüsse-lungsmodus von SGEasy**	**Status der beiden speziellen Partitionen**
Windows 2000	Partitionsweise	Die Partitionen ist **nicht verschlüsselt**. Vorteil: Die Lenovo-Werkseinstellungen können von der lokalen Festplatte wiederhergestellt werden. Nachteil: Hacker können eine unverschlüsselte Rescue and Recovery-Bootumgebung manipulieren.
Windows XP	Partitionsweise Standard Bootschutz	
Windows 2000	Standard Bootschutz	Die Partitionen **werden verschlüsselt**. Vorteil: Die Bootumgebung ist verschlüsselt. Sie kann nur geändert werden, wenn das SafeGuard Easy-Passwort bekannt ist. Nachteil: Die Lenovo-Werkseinstellungen können nicht von der lokalen Festplatte wiederhergestellt werden. **Für das Zurücksetzen auf die Werkseinstellungen benötigen Sie eine spezielle CD/DVD. Der Support von Lenovo schickt Ihnen diese Medien auf Anfrage gerne zu.** Alternativ kann die Festplatte über die Notfalldis-kette und das DOS-Tool `Sgeasy.exe` entschlüs-selt werden (= Deinstallation von SafeGuard Easy).

Utimaco empfiehlt, entweder die Service Partition zu verschlüsseln oder stattdessen die Rescue and Recovery-Umgebung in die virtuelle Partition zu installieren. Die virtuelle Partition ist immer geschützt, sobald das Windows-Systemlaufwerk verschlüsselt ist!

24.10 Was tun, wenn...

... nach dem Neustart des PCs auf dem Bildschirm eine SafeGuard Easy Viruswarnung angezeigt wird?

Mögliche Gründe dafür sind:

1. *Sie haben einen Virus auf Ihrem System.*

   Kontaktieren Sie bitte umgehend Ihren Systemadministrator.

2. *Sie haben vergessen, nach der Installation, Modifikation oder Deinstallation von Rescue and Recovery den MBR mit dem Kommando* `MBRsync.exe` *zu synchronisieren.*

   SafeGuard Easy erkennt Modifikationen am MBR und reagiert darauf in der Standardeinstellung mit einer Menüanzeige (siehe 'Master Boot Record'). Wenn Sie sich sicher sind, dass die Meldung durch Rescue and Recovery ausgelöst wurde, wählen Sie im Menü bitte „Übernehmen“.
   Nur der Benutzer "SYSTEM" sieht die Menüanzeige.

...das Dateisystem beschädigt ist?
Hier genügt in der Regel ein einfaches Einspielen einer Sicherungskopie (mit SafeGuard Easy) mit Rescue and Recovery.

Alternativ kann die Festplatte über die Notfalldiskette und das DOS-Tool `Sgeasy.exe` entschlüsselt werden (=Deinstallation von SafeGuard Easy). Die Festplatte ist dann wieder im Klartext vorhanden und kann mit üblichen Tools für die Daterettung bearbeitet werden. Darf der Benutzer aufgrund fehlender Rechte SafeGuard Easy nicht deinstallieren, hilft das SafeGuard Easy Challenge/Response-Verfahren und erteilt dem Benutzer temporär das Recht dazu.

... die Festplatte physikalisch beschädigt ist?
Wenn die Festplatte physikalisch beschädigt ist und nicht einmal mit `Sgeasy.exe` entschlüsselt werden kann, kontaktiert Utimaco auf Kundenwunsch Partner, die darauf spezialisiert sind, physikalisch beschädigte Laufwerk zu retten.

...der SafeGuard Easy-Systemkern beschädigt ist?
Bei geringfügigen Fehlern wie einem überschriebenen MBR repariert `Sgeasy.exe` den MBR oder spielt einen zuvor gesicherten Backup des Systemkerns ein.

...die Initialverschlüsselung abgebrochen wurde und Windows nicht mehr gebootet werden kann?
Wenden Sie sich in diesem Fall an den Utimaco Support.

...die endgültige Entschlüsselung abgebrochen wurde und Windows nicht mehr gebootet werden kann?
Wenden Sie sich in diesem Fall an den Utimaco Support.

25 Kompatibilität zur Computrace Software der Absolute Software Corp.

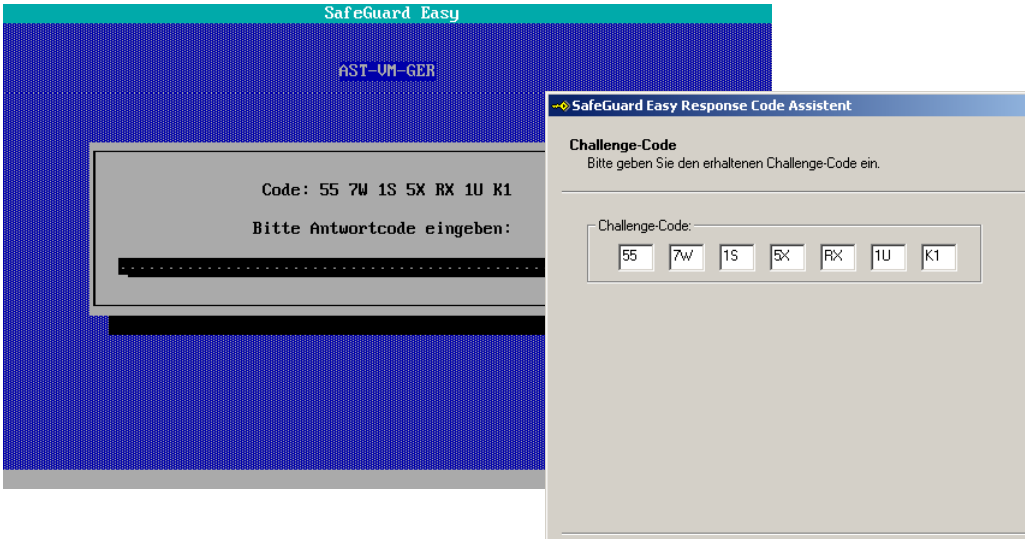
Lenovo schützt seine neuen Thinkpad Notebooks mit zahlreichen Sicherheitsfeatures (u.a. SafeGuard Easy und SafeGuard PrivateDisk) und garantiert seinen Benutzern damit hohe mobile Sicherheit. Neben den Produkten der SafeGuard Familie ist auch Computrace der Absolute Software Corp. auf verschiedenen Lenovo Notebooks vorinstalliert.

Computrace hilft, ein Notebook im Fall eines Diebstahls wieder aufzuspüren, sobald sich der gestohlene PC mit dem Internet verbindet. Zudem können auf Wunsch des rechtmäßigen Nutzers vertrauliche Daten vom gestohlenen Rechner gelöscht werden. Lenovo integriert Computrace als bereits in die PC-Hardware (persistent BIOS based Agent).

Durch die Kompatibilität mit SafeGuard Easy funktioniert die Computrace-Software mit verschlüsselten Festplatten.

SafeGuard Easy ist kompatibel zu Computrace Complete mit "BIOS Persistence", nicht aber mit "Software Persistence".

26 Fernwartung (Challenge/ Response)

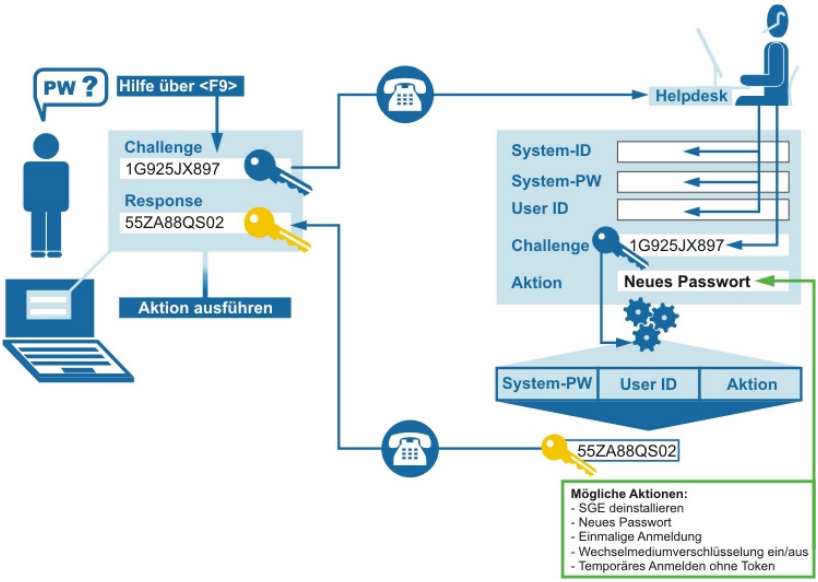


SafeGuard Easy bietet das Challenge/Response-Verfahren zum Zurücksetzen „vergessener“ SafeGuard Easy- oder Token-Passwörter.

Challenge/Response ist sehr sicher und effizient:

- Es werden keine vertraulichen Daten ausgetauscht.
- Das „Belauschen“ bzw. die Verwendung „abgehörter Daten“ ist nutzlos.
- Ist auch für Geräte ohne Netzwerkanbindung verwendbar.
- Der Benutzer kann in kürzester Zeit seine Arbeit wieder aufnehmen.

26.1 Funktionsweise



Benötigt ein Benutzer (entfernter Benutzer) Hilfe, muss er einen Challenge Code erzeugen. Dieser Challenge Code wird auf seinem PC als ASCII Zeichen-Kette angezeigt. Der entfernte Benutzer ruft anschließend beim Helpdesk an und gibt seine Benutzerinformationen und den Challenge Code an. Der Helpdesk startet den SafeGuard Easy Response Code Assistenten und erzeugt dann einen Response Code. Der Helpdesk teilt den Response Code per Telefon oder SMS dem entfernten Benutzer mit, und dieser kann nach der Eingabe des Response Codes sein Passwort neu setzen.

Generell können über Challenge/Response folgende Sonderrechte erteilt werden:

- Neues SafeGuard Easy-Benutzerpasswort setzen (wenn das Alte vergessen wurde)
- SafeGuard Easy deinstallieren
- Einmalige Anmeldung (bspw. für Wartungsarbeiten)
- Recht zum Schalten der Diskettenverschlüsselung temporär vergeben (für die Dauer einer Anmeldung)
- Anmeldung ohne Token erlauben
- Erlaubnis, einen Token auszustellen

Der Response Code Assistent kann auf einem PC oder auf dem PDA des Helpdesk-Mitarbeiters installiert sein.

26.1.1 Response Code Assistenten für PDA installieren

Die PDA-Version des Response Code Assistenten finden Sie auf der SafeGuard Easy-CD.

1. Kopieren Sie die Datei `SGE_CRW.PPC30_ARM.cab` aus dem \TOOLS Verzeichnis der SafeGuard Easy CD auf den PDA.
2. Rufen Sie `SGE_CRW.PPC30_ARM.cab` über den PDA Datei-Explorer auf. Die Installation wird sofort ausgeführt.
3. Nach der Installation ist ein Soft Reset nötig.

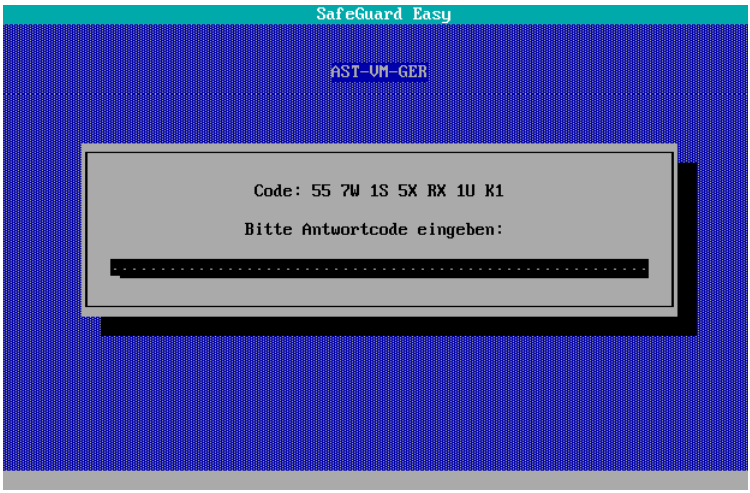
SafeGuard PDA muss auf dem PDA installiert sein.

26.2 Challenge Code erzeugen

Der Challenge Code wird vom Benutzer erzeugt, der z.B. sein SafeGuard Easy-Passwort vergessen hat. Abhängig von der Art des Systemstarts ergeben sich unterschiedliche Vorgehensweisen beim Erzeugen des Challenge Codes:

Systemstart mit Pre-Boot Authentisierung

Beim **Systemstart mit Pre-Boot Authentisierung** muss der Benutzer seinen SafeGuard Easy-Benutzernamen an der Pre-Boot Authentisierung eingeben und anschließend in das Passwortfeld wechseln. Nach Drücken von [F9] wird der Challenge Code angezeigt.



Systemstart ohne Pre-Boot Authentisierung

Beim **Systemstart ohne Pre-Boot Authentisierung** erscheint beim Booten des Rechners für wenige Sekunden ein Diskettensymbol in der linken oberen Ecke des Bildschirms. Der Benutzer drückt nun während dieses Zeitraums die Taste [F2]. Der Anmeldedialog der Pre-Boot Authentisierung erscheint, und der Benutzer gibt seinen SafeGuard Easy-Benutzernamen an der Pre-Boot Authentisierung ein und wechselt ins Passwortfeld. Nach Drücken von [F9] wird der Challenge Code angezeigt.

Sonderfall Deinstallation

Um SafeGuard Easy per Challenge/Response zu deinstallieren, muss der Challenge Code über den Deinstallationsdialog (Programme / Systemsteuerung / Software / SafeGuard Easy / Entfernen) erzeugt werden. Eine Deinstallation von SafeGuard Easy mit Hilfe des Challenge/Response-Verfahrens kann **nicht in der Pre-Boot Authentisierung** begonnen werden.

26.3 Response Code

Der Administrator bzw. Helpdesk-Mitarbeiter erzeugt den Response Code mit dem Response Code Assistenten.

Wer den Response Code erzeugt, muss die Daten eines SafeGuard Easy-Benutzerprofils am entfernten Benutzer-PC kennen, z.B. die Daten des Benutzerprofils „Helpdesk“. „Helpdesk“ muss am Benutzer-PC wenigstens über die gleichen Rechte wie der anfragende SafeGuard Easy-Benutzer verfügen.

Damit das Benutzerprofil „Helpdesk“ bestimmte Sonderrechte gewähren kann, benötigt es für die jeweilige Aktion folgende Benutzerrechte:

Geplante Helpdesk-Aktion auf einem Benutzer-PC	Nötiges SafeGuard Easy Recht
SafeGuard Easy deinstallieren	SafeGuard Easy deinstallieren
Neues Passwort festlegen	Benutzereinstellungen ändern
Einmalige Anmeldung	Benutzereinstellungen ändern
Recht zum Schalten der Diskettenverschlüsselung temporär vergeben	Diskettenverschlüsselung schalten
Anmeldung ohne Token für X Anmeldungen	Benutzereinstellungen ändern
Erlaubnis zum Ausstellen eines Token erteilen	---

26.3.1 Response Code erzeugen

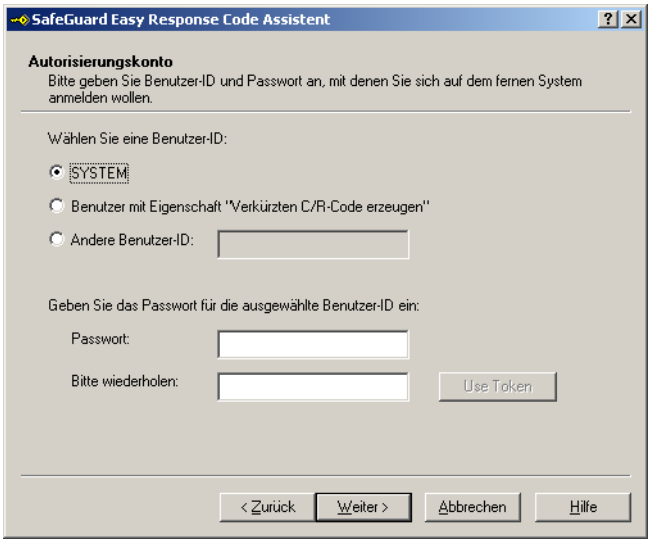
> ***HINWEIS:***
> Auf einem PC muss der SafeGuard Easy Response Code Assistent installiert sein.
>
> Auf einem PDA muss SafeGuard PDA und die PDA-Version des Response Code Assistenten installiert sein.

Starten Sie den Response Code Assistenten über **Programme / SafeGuard Easy / Utimaco / Response Code Assistent**. Der erste Dialog zeigt Informationen über den Assistenten an.

Bestätigen Sie in der Folge richtige Eingaben mit [Weiter].

Autorisierungskonto

Im Dialog „Autorisierungskonto“ wählen Sie den SafeGuard Easy-Benutzer, mit dem Sie sich am System des entfernten Benutzers anmelden wollen.


SafeGuard Easy Response Code Assistent
Autorisierungskonto
Bitte geben Sie Benutzer-ID und Passwort an, mit denen Sie sich auf dem fernen System anmelden wollen.
Wählen Sie eine Benutzer-ID:
SYSTEM
Benutzer mit Eigenschaft "Verkürzten C/R-Code erzeugen"
Andere Benutzer-ID:
Geben Sie das Passwort für die ausgewählte Benutzer-ID ein:
Passwort:
Bitte wiederholen:
Use Token
< Zurück
Weiter >
Abbrechen
Hilfe

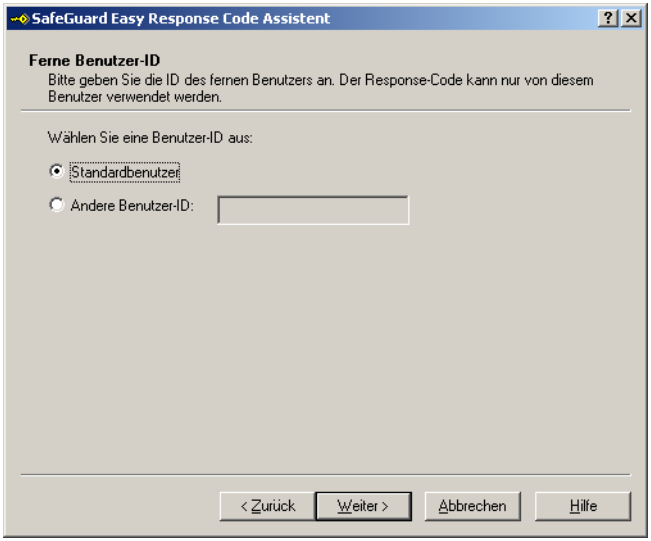
- **SYSTEM:**
  Benutzername des SafeGuard Easy-Benutzers SYSTEM; SYSTEM darf alle Sonderrechte gewähren.
- **Benutzer mit Eigenschaft „Vereinfachte Fern-Anmeldung“:**
  Benutzer, dem auf dem Zielsystem diese Eigenschaft zugeordnet wurde. Er muss mindestens über die Rechte des fernen Benutzers verfügen.
- **Andere Benutzer-ID:**
  Benutzernamen eines beliebigen SafeGuard Easy-Benutzers, der ein Sonderrecht gewähren darf.
- **Schaltfläche „Token benutzen“**
  Liest das SafeGuard Easy Passwort des angegebenen Benutzers vom Token, wenn sich der Benutzer mit Token in der PBA angemeldet hat.

Der hier gewählte Benutzernamen beeinflusst die Länge des Response Codes, der später erzeugt wird. Je länger der Response Code, desto höher ist die Gefahr, dass beim Eintippen bzw. Übermitteln an den Benutzer Fehler auftreten.

Benutzer-ID	Länge der Response (Zeichen)
SYSTEM	30
Benutzer mit Eigenschaft „Verkürzten C/R Code erzeugen“	30
Andere Benutzer-ID	56

Ferne Benutzer-ID

Im nächsten Dialog wählen Sie den SafeGuard Easy Benutzernamen des entfernten Benutzers. Fragen Sie den Benutzer, mit welchen Zugangsdaten er sich üblicherweise an seinem Rechner anmeldet.

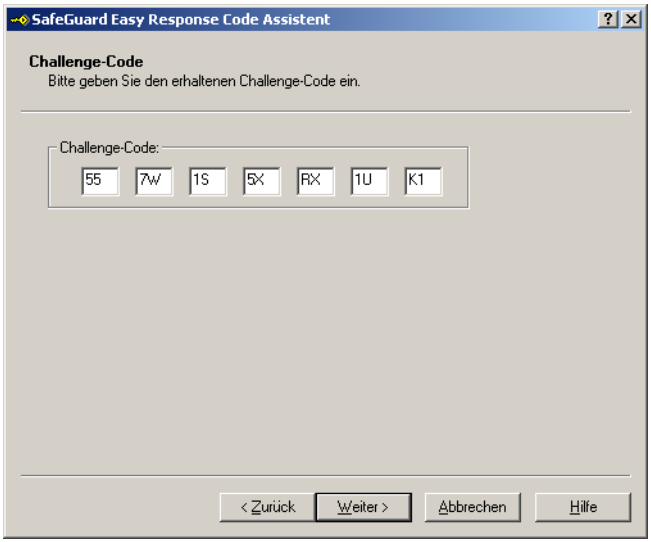

SafeGuard Easy Response Code Assistent
Ferne Benutzer-ID
Bitte geben Sie die ID des fernen Benutzers an. Der Response-Code kann nur von diesem Benutzer verwendet werden.
Wählen Sie eine Benutzer-ID aus:
Standardbenutzer
Andere Benutzer-ID:
< Zurück
Weiter >
Abbrechen
Hilfe

- **Standardbenutzer:**
  Benutzer meldet sich nur mit seinem SafeGuard Easy-Passwort an, d.h. er ist auf dem Zielsystem als Standardbenutzer registriert und kennt demzufolge den Benutzernamen nicht.

- **Andere Benutzer-ID:**
  Benutzer meldet sich mit SafeGuard Easy-Benutzernamen und Passwort an. Der SafeGuard Easy-Benutzernamen ist demzufolge bekannt. Tragen Sie ihn in das Feld ein.

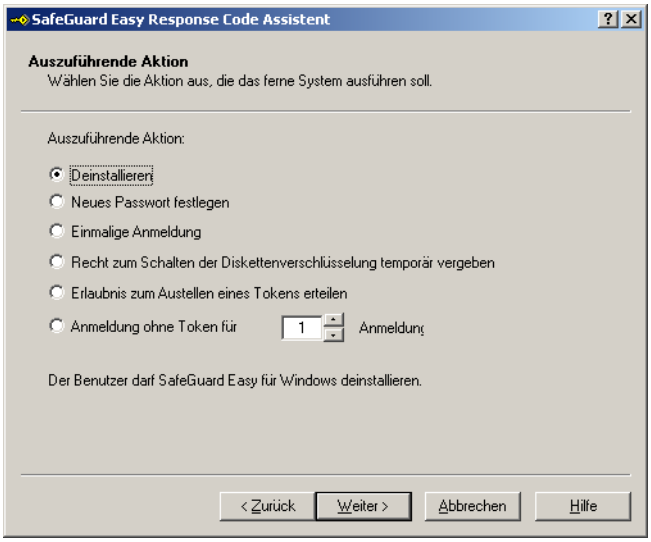
Challenge Code

Im nächsten Dialog geben Sie bitte in die paarweise getrennten Felder den Code ein, den Ihnen der entfernte Benutzer (z.B. per Telefon) mitteilt. Der **Challenge Code** wird dem Benutzer auf seinem PC als ASCII-Zeichenkette (14 Zeichen) angezeigt.



Auszuführende Aktion

Im nächsten Dialog wählen Sie die **Aktion**, die dem entfernten Benutzer erlaubt werden soll:



Eine der folgende Aktionen kann ausgeführt werden:

- **Deinstallieren**
  Benutzer darf SafeGuard Easy deinstallieren. Diese Art der Deinstallation ist nur sinnvoll, wenn der Administrator nicht vor Ort ist.

- **Neues Passwort festlegen**
  Benutzer darf sein Passwort ändern, z.B. wenn er das alte Passwort vergessen hat oder sich durch mehrmalige falsche Passworteingabe die Wartezeit an der Pre-Boot Authentisierung zu sehr erhöht hat.

  Das Passwort des Benutzers SYSTEM kann nicht per Challenge/Response neu vergeben werden.

- **Einmalige Anmeldung**
  Benutzer erhält er für die Dauer einer Arbeitssitzung Zugang zum betreffenden Rechner.

  Dies ist sinnvoll, wenn bspw. ein Techniker Wartungsarbeiten durchführt.

- **Recht zum Schalten der Diskettenverschlüsselung temporär vergeben**
  Der Benutzer darf für die Dauer einer Arbeitssitzung die Diskettenverschlüsselung ein- bzw. ausschalten. Der Schlüssel für die Diskettenverschlüsselung muss bereits gesetzt sein.

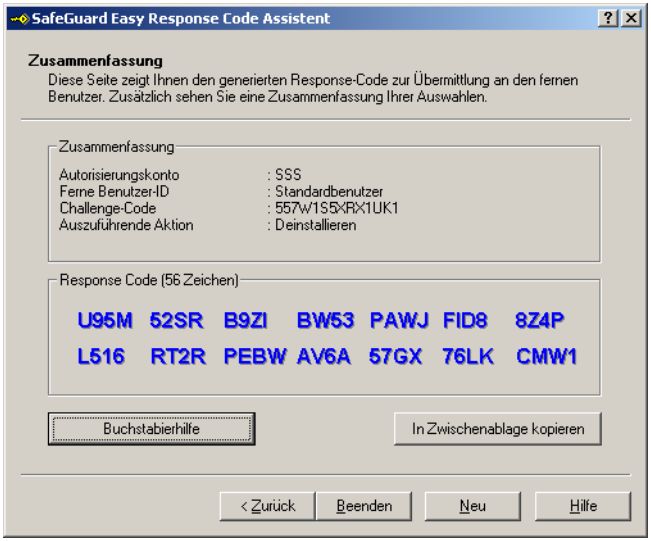
- **Erlaubnis zum Ausstellen eines Token erteilen**
  Der Benutzer darf einmalig einen Token ausstellen. Diese Option ist relevant, wenn ein Token nur über ein Challenge/Response Verfahren ausgestellt werden kann (Ausstellungsmodus: „Externe Erlaubnis erforderlich").

- **Anmeldung ohne Token für „X“ Anmeldungen**
  Der Benutzer darf sich X-mal (Maximum: 12) ohne Token anmelden. Diese Aktion kommt zum Einsatz, wenn der Token zuhause vergessen wurde, der Benutzer aber nur mit Token Zugang zu seinem PC erhält.

Mit Bestätigen der Eingaben wird der Response Code erzeugt.

Zusammenfassung

Im letzten Dialog erhalten Sie einen kompletten Überblick über die von Ihnen in den vorangegangenen Dialogen des Response Code Assistenten getroffenen Einstellungen. Zusätzlich wird folgendes angezeigt:


SafeGuard Easy Response Code Assistent
Zusammenfassung
Diese Seite zeigt Ihnen den generierten Response-Code zur Übermittlung an den fernen Benutzer. Zusätzlich sehen Sie eine Zusammenfassung Ihrer Auswahlen.
Zusammenfassung
Autorisierungskonto : SSS
Ferne Benutzer-ID : Standardbenutzer
Challenge-Code : 557W1S5XRX1UK1
Auszuführende Aktion : Deinstallieren
Response Code (56 Zeichen)
U95M 52SR B9ZI BW53 PAWJ FID8 8Z4P
L516 RT2R PEBW AV6A 57GX 76LK CMW1
Buchstabierhilfe
In Zwischenablage kopieren
< Zurück
Beenden
Neu
Hilfe

Response Code

Zeigt den erzeugten Response Code in blauer Schrift an. Dieser Code muss an den entfernten Benutzer gegeben werde. Der entfernte Benutzer trägt den Response Code in die dafür vorgesehenen Felder ein. Der Response Code ist nur einmal gültig! Für jeden Request muss ein neuer erzeugt werden.

In Zwischenablage kopieren

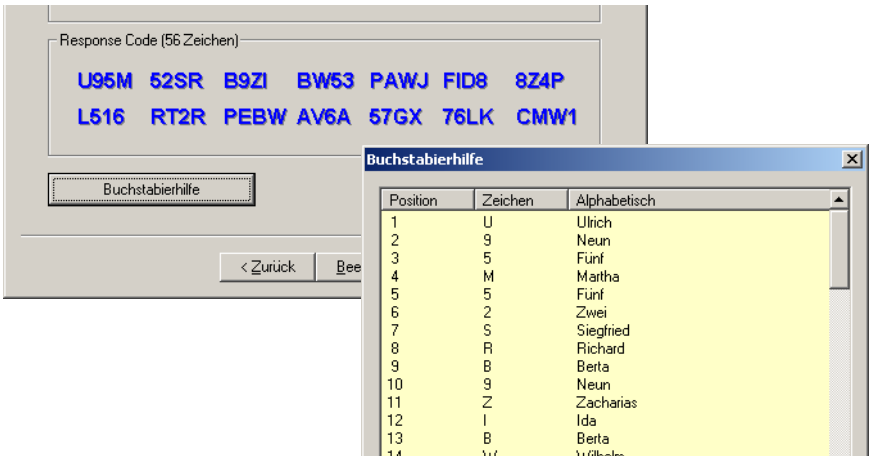
Der Response Code wird in die Zwischenablage kopiert und kann in einen beliebigen Texteditor eingefügt werden. Dieses Feature erlaubt z.B. den Response Code einfach per SMS oder E-Mail an den Benutzer zu verschicken.

Sind alle Angaben korrekt und der Benutzer konnte die erforderlichen Aktionen ausführen, wird der Response Code Assistent durch einen Klick auf **Beenden** geschlossen. Durch Klicken auf **Neu** werden alle Angaben gelöscht und Sie können eine neue/weitere Response erzeugen.

Buchstabierhilfe

Um das Übermitteln des Codes an den Benutzer zu erleichtern und Fehler zu vermeiden, gibt es im Response Code Assistenten eine Buchstabierhilfe.

Drücken Sie die Schaltfläche [Buchstabierhilfe], erscheint ein in drei Spalten gegliedertes Fenster mit den jeweiligen Spaltenüberschriften. Unter „Position“ sehen Sie, an welcher Stelle das Zeichen innerhalb des Codes steht. Nachfragen können somit sofort ohne größeren Zeitaufwand (wie z.B. Abzählen der Stellen) beantwortet werden. Welches Zeichen anzugeben ist, sehen Sie unter der gleichnamigen Rubrik. „Alphabetisch“ gibt an, mit welchem Wort die Zeichen „verknüpft“ werden können, um Verwechslungen zu vermeiden. In der Regel werden Vornamen verwendet, deren erster Buchstabe dann in die Codefelder eingetragen wird. Im Fenster wird bereits der tatsächliche Response Code dargestellt. Sie müssen diesen nur von oben nach unter vorlesen.



26.4 Erweiterung des Challenge/ Response Konzepts

Zusätzlich zum Standard-Verfahren gibt es noch verschiedene software- und hardwarebasierende Challenge/Response-Lösungen.

26.4.1 Helpdesk-Konsole

Für große Umgebungen, in denen die Helpdesk Mitarbeiter die Master Passwörter der SafeGuard Easy Clients nicht kennen sollen, kann das Challenge-Response System auf Helpdesk Seite mit einem kryptographischen Hardwaremodul (CryptoServer) oder einer software-basierenden Lösung erweitert werden.

Hardware-basierende Helpdesk-Konsole

Bei Verwendung des CryptoServer 2000 werden die Passwörter vom SafeGuard Easy Administrator einmalig in den CryptoServer 2000 eingegeben und dort sicher gespeichert. Den Mitarbeitern des Helpdesk sind diese Passwörter nicht bekannt.

Der Response Code wird nun innerhalb des CryptoServer 2000 erzeugt. Der Helpdesk Mitarbeiter kann auf diese Weise zu gegebenen Benutzerdaten (Name, Challenge Code) einen Response Code erzeugen ohne selbst das Passwort des SafeGuard Easy Administrators zu kennen. Jeder Helpdesk Mitarbeiter erhält dazu vom Systemadministrator des CryptoServer 2000 einen Account (Benutzername, Passwort) auf dem CryptoServer, der ihn berechtigt, einen Response Code zu erzeugen. Dieser Account kann jederzeit gelöscht werden (z.B. bei Ausscheiden des Mitarbeiters), so dass der betreffende Mitarbeiter nicht länger in der Lage ist, auf den CryptoServer 2000 zuzugreifen.

Die hardwarebasierende Helpdesk-Konsole ist als separates Add-on erhältlich.

Zentrale Helpdesk-Konsole

Die zentrale Helpdesk-Konsole funktioniert ähnlich wie die CryptoServer-Lösung. Auch hier kennen die Helpdesk-Mitarbeiter die administrativen SafeGuard Easy Passwörter nicht.

Bei dieser softwarebasierenden Variante (Webinterface) ist die Information, die notwendig ist, um eine Response zu erzeugen, in einer geschützten (mit AES-256 verschlüsselten) Datenbank auf einem PC gespeichert, auf dem der Microsoft Internet Information Service läuft. Zum Erzeugen von Response Code authentisieren sich die Helpdesk-Mitarbeiter auf der Webseite am Internet Information Server.

Die zentrale Helpdesk-Konsole ist als separates Add-on erhältlich.

26.4.2 Web Self Help

Wichtigster Vorteil der webbasierten Hilfe ist, dass Benutzer ohne Einbindung des Helpdesk vergessene SafeGuard Easy Passwörter zurücksetzen können. Damit ein Benutzer in Eigenverantwortung sein Passwort neu setzen darf, muss er sich zunächst an einer zentralen Datenbank registrieren. Die Registrierung erfolgt über einen speziellen Mechanismus: Der Benutzer gibt für eine bestimmte Anzahl frei wählbarer Fragen seine Antworten ein. Diese Antworten werden in der Datenbank gespeichert. Der registrierte Benutzer wird vom Administrator freigegeben und erhält eine Mail mit einer PIN. Will der Benutzer anschließend über die Web-based Self Help einen Response Code für sein registriertes SafeGuard Easy Profil erzeugen, muss er die PIN und die korrekten Antworten eingeben.

Das Verfahren ist webbasierend und damit beinahe uneingeschränkt für Benutzer zugänglich, es ist auch keine zusätzliche Software auf dem Client nötig.

Die webbasierte Passwort-Selbsthilfe ist als separates Add-on erhältlich.

26.4.3 VOICE.TRUST

Eine andere mögliche Erweiterung des Challenge-Response Systems ist die Einrichtung eines biometrischen Servers von VOICE.TRUST mit Plug-in für SafeGuard Easy oder SafeGuard PDA. Der VOICE.TRUST Server kann anrufende Benutzer anhand ihrer Stimme (Voiceprint) authentisieren, und den gesamten Challenge-Response Vorgang mit dem Benutzer über Spracherkennung und -synthese rund um die Uhr selbständig ausführen. Menschliche Helpdesk Mitarbeiter sind nur noch in Ausnahmefällen nötig und dadurch von Routineaufgaben wie dem Zurücksetzen von Passwörtern entlastet.

Bitte wenden Sie sich an Ihren lokalen SafeGuard Easy Anbieter für Informationen über die Erweiterungen zum Challenge/Response- Verfahren.

27 Notfallmedien erstellen und Systemkern sichern

Wenn Ihr Rechner bei verschlüsselter Festplatte SafeGuard Easy-Fehlermeldungen anzeigt, kann in den meisten aller Fälle der Systemkern von SafeGuard Easy nicht gefunden werden. Im Systemkern befinden sich die Treiber für SafeGuard Easy und der Master Boot Record.

Aufgetretene Fehler können jedoch häufig mit Einspielen eines gesicherten aktuellen Systemkerns behoben werden. Für das Einspielen des Systemkerns muss der Benutzer allerdings neben einem intakten Systemkern ein **Notfallmedium (Diskette, CD oder USB-Stick)** zur Hand haben. Auf diesem Medium befinden sich der gesicherte Systemkern und Dateien, die beim Beheben von SafeGuard Easy Fehlern helfen.

Da Sie im Fall eines Systemdefekts wahrscheinlich nicht auf die Festplatte zugreifen können, sollte der Systemkern immer auf einer Diskette, einem Wechselmedium oder dem Netzlaufwerk abgelegt sein.

HINWEIS:
Weitere Informationen zu diesem Thema erhalten Sie in der Utimaco-Wissensdatenbank http://www.utimaco.de/myutimaco.

Nutzen Sie bitte die Suchfunktion der Wissensdatenbank, um nach Stichworten wie „Notfall“ oder „Emergency“ zu suchen.

27.1 Notfalldiskette erstellen

Die Notfalldiskette erstellt der „Assistent für Notfalldiskette“, der nach jeder Standard-Installation auf einem Client vorhanden ist. Sind Disketten-/Wechselmedienlaufwerke verschlüsselt, wird die Verschlüsselung während der Erstellung der Notfalldiskette ausgeschaltet.

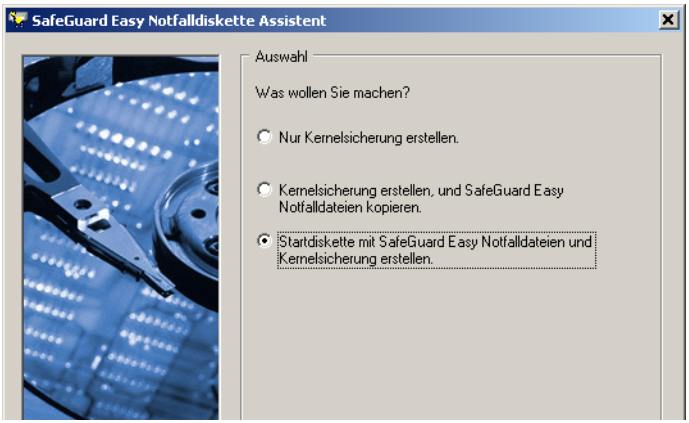
Damit auf einer Notfalldiskette immer der aktuellste Systemkern vorhanden ist, sollte eine Sicherung nach jeder signifikanten Änderung wie etwa der Änderung des Verschlüsselungsstatus durchgeführt werden. Es ist über eine Option im Notfallassistenten konfigurierbar, dass Benutzer in regelmäßigen Abständen aufgefordert werden, den Systemkern zu sichern. Dieser muss dann auf die Notfalldiskette kopiert werden.

27.1.1 Notfallassistenten starten

Der Notfallassistent startet automatisch nach dem ersten Neustart nach der Installation von SafeGuard Easy, ist aber auch aufrufbar über **Programme/Utimaco/SafeGuard Easy/Assistent für Notfalldiskette**.

Bestätigen Sie alle richtigen Angaben im Assistenten mit [Weiter].

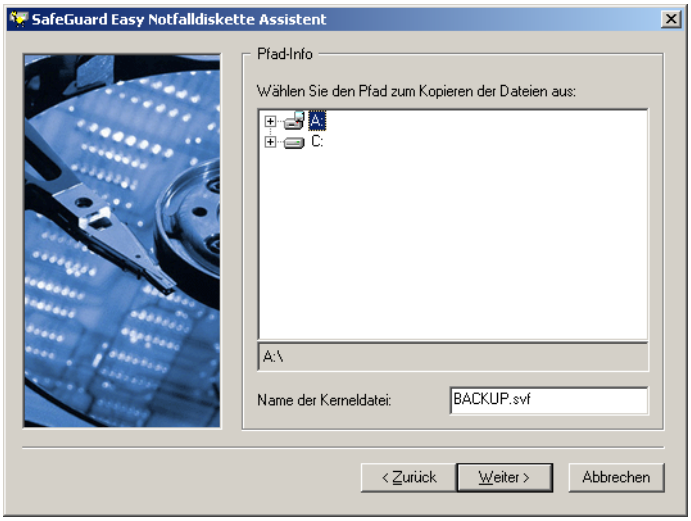
1. Ist der Assistent gestartet, legen Sie im zweiten Dialog fest, welche Dateien auf der Notfalldiskette gespeichert werden sollen.


SafeGuard Easy Notfalldiskette Assistent
Auswahl
Was wollen Sie machen?
Nur Kernelsicherung erstellen.
Kernelsicherung erstellen, und SafeGuard Easy Notfalldateien kopieren.
Startdiskette mit SafeGuard Easy Notfalldateien und Kernelsicherung erstellen.

Folgende Optionen stehen zur Auswahl:

- **Nur Kernelsicherung erstellen**
  Sichert den kompletten Systemkern (Treiber für SafeGuard Easy und den Master Boot Record) in eine Datei.
- **Kernelsicherung erstellen und SafeGuard Easy Notfalldateien kopieren**
  Kopiert den Systemkern und die Notfalldateien.
- **Startdiskette mit SafeGuard Easy Notfalldateien und Kernelsicherung erstellen**
  Erstellt eine bootfähige Rettungsdiskette mit einer FreeDOS-Version, Systemkern und Notfalldateien.

Anschließend wählen Sie aus, wo die Daten (Systemkern und Notfalldateien) gespeichert werden.



Im Pfad-Info Feld bestimmen Sie, wo Systemkern und Notfalldateien (wenn ausgewählt) gesichert werden sollen. Unter Name der Kerneldatei geben Sie für den Systemkern einen Namen an. Voreinstellung ist `Backup.svf`, Name und die Extension SVF können aber geändert werden. Es ist auch möglich, den Systemkern auf der Festplatte oder einem Netzlaufwerk abzulegen.

Da Sie im Fall eines Systemdefekts wahrscheinlich nicht auf die Festplatte zugreifen können, sollte der Systemkern samt Notfalldateien immer auf einer Diskette, einem Wechselmedium oder dem Netzlaufwerk abgelegt sein.

2. Stellen Sie im Dialog *Reminder* ein, in welchen Zeitabständen Sie an die Systemkernsicherung erinnert werden möchten.

   Damit bei auftretenden Systemfehlern immer die aktuellste Systemkern Version zur Hand ist, ist es ratsam, regelmäßige Sicherungen durchzuführen.

SafeGuard Easy Notfalldiskette Assistent
Reminder
Der Vorgang wurde erfolgreich beendet. Wenn Sie gerade die Sicherung der Kerneldatei auf eine Diskette oder auf ein anderes wechselbares Medium erstellt haben, beschriften Sie bitte entsprechend das Medium, und bewahren Sie es in einem sicheren Ort auf.
Eine regelmäßige Sicherung des SafeGuard Easy Sicherheitskernel wird stark empfohlen. Wenn Sie das nicht machen und das Kernel beschädigt wird, könnten alle verschlüsselte Daten verlorengehen.
Starten des Assistent alle
30
Tage.
< Zurück
Beenden
Abbrechen

27.1.2 Systemkern per Kommandozeile sichern

Sie können den Systemkern auch von der Kommandozeile sichern, und zwar über

```
SGEBACK.EXE /f:<Pfad/Dateiname> | /S | /?
```

/f: Gibt den Pfad und Dateinamen der Kernelsicherung an
Name und Extension der Zieldatei sind frei wählbar.

/S Schickt die im Parameter /f definierte Kernelsicherung an den SafeGuard Easy Server

/?Zeigt diese Hilfe

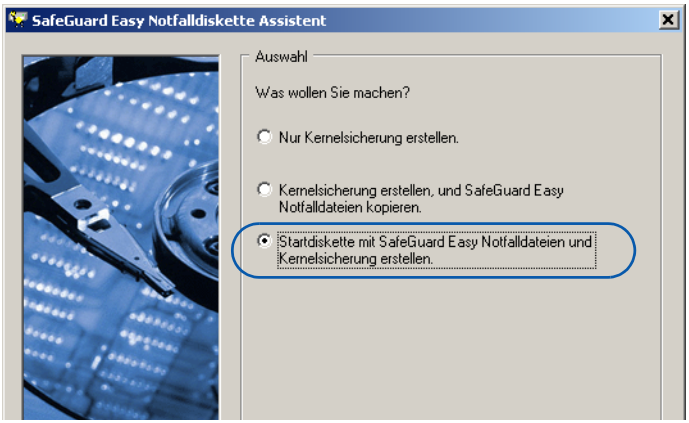
27.1.3 SafeGuard Easy Notfalldateien manuell auf Diskette sichern

Sie können die Notfalldateien auch manuell auf eine Diskette sichern. Kopieren Sie folgende Dateien aus dem Installationsverzeichnis von SafeGuard Easy:

- SGEASY.exe
- Sgeasy.hmf
- Sgecrypt.mod
- Sgenls.mod
- Sgekrnl.mod

27.2 Bootfähige Notfalldiskette erstellen

Als zusätzliche Option bietet der Notfallassistent an, eine bootfähige Startdiskette samt Systemkern, Notfalltools und Treiberdateien für das Tastaturlayout zu erstellen. Dies ist eine komfortable Möglichkeit, Bootdiskette und SafeGuard Easy Notfalldiskette zu kombinieren.


SafeGuard Easy Notfalldiskette Assistent
Auswahl
Was wollen Sie machen?
Nur Kernelsicherung erstellen.
Kernelsicherung erstellen, und SafeGuard Easy Notfalldateien kopieren.
Startdiskette mit SafeGuard Easy Notfalldateien und Kernelsicherung erstellen.

So erstellen Sie eine bootfähige Notfalldiskette:

1. Formatierte Diskette einlegen und Notfallassistenten starten.
2. Option „Startdiskette mit SafeGuard Easy Notfalldateien und Kernelsicherung erstellen“ auswählen.

Utimaco empfiehlt, beim erstmaligen Sichern des Systemkerns eine bootfähige Startdiskette zu erstellen und sobald der Systemkern geändert wird, nur diesen zu aktualisieren.

27.3 Bootfähige Notfall-CD erstellen

Mobile Geräte wie Notebooks besitzen heutzutage i.d.R. kein Diskettenlaufwerk mehr. SafeGuard Easy erlaubt deswegen auch einen Notfallstart von einer CD.

So erstellen Sie eine bootfähige Notfall-CD:

1. Boot-Image-Datei `Floppy.iso` aus dem Verzeichnis \TOOLS auf der Festplatte speichern und mit Hilfe eines handelsüblichen Brennprogramms auf eine CD brennen.
   Die Iso-Datei enthält die komplette Boot-Diskette, wie sie vom Notfallassistenten erstellt wird, mit Ausnahme der Systemkernsicherung.
2. Systemkernsicherung erstellen über den „Assistent für Notfalldiskette“. Systemkernsicherung entweder auf der CD selbst oder aber auf einem externen Klartextmedium speichern, auf das im Notfall Zugriff möglich ist.

Stellen Sie im BIOS sicher, dass das System von CD startet.

Das erfolgreiche Booten über CD ist abhängig vom BIOS Support des PC!

27.4 Bootfähigen Notfall-USB-Stick erstellen

Der USB-Stick muss auf Ihrem System bootfähig sein!

So erstellen Sie einen bootfähigen Notfall-USB-Stick:

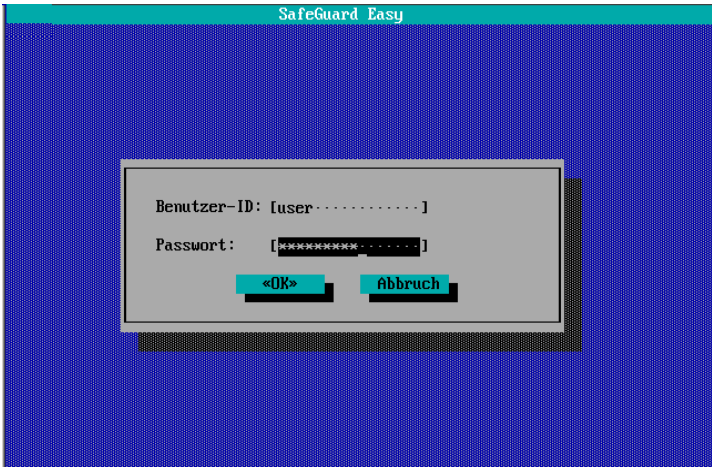
1. USB-Stick so vorbereiten, dass er bootfähig ist.
2. SafeGuard Easy Notfalldateien auf den Stick kopieren.

Das erfolgreiche Booten über USB-Stick ist abhängig vom BIOS Support des PC!

27.5 Notfallstart durchführen

Tritt ein Systemfehler bei verschlüsselter Festplatte auf, gehen Sie folgendermaßen vor:

1. PC starten und von Notfalldiskette/-CD/-USB-Stick booten.
2. Das Notfallprogramm Sgeasy.exe aufrufen, wenn es nicht automatisch gestartet wird.
3. SafeGuard Easy-Zugangsdaten in den Anmeldebildschirm eingeben. Angaben mit [OK] bestätigen.



4. Es erscheint dann ein Menü mit den Punkten *Deinstallieren, Sichern, Restaurieren*, *Reparieren.*

27.5.1 Systemkern restaurieren

Das Restaurieren des Systemkerns setzt das Vorhandensein eines gültigen Systemkerns der Arbeitsstation voraus. Wenn es eine Sicherung gibt, werden der MBR und der SafeGuard Easy Systemkern einfach anhand dieses Datenbackups auf der Arbeitsstation wiederhergestellt.

Diese Funktion darf ***nicht*** ausgeführt werden, wenn

- SafeGuard Easy vorher deinstalliert wurde
- die Systemkernsicherung nicht dem aktuellen Stand entspricht. Dies trifft zu, wenn z.B. zwischen dem Sichern des Systemkerns und dem Restaurieren der Verschlüsselungsstatus der Festplatte(n) geändert wurde.

Alle SafeGuard Easy-Benutzer eines PCs dürfen einen gesicherten Systemkern wieder einspielen.

27.5.2 Systemkern reparieren

Im Gegensatz zu „Restaurieren“ funktioniert ein Reparieren auch ohne Sicherungskopie des Systemkerns. Die Reparieren-Funktion durchsucht die komplette Festplatte nach dem SafeGuard Easy Systemkern und versucht ihn wiederherzustellen (keine Erfolgsgarantie!).

Diese Funktion wird nur dann benötigt, wenn

- keine Sicherung des Systemkerns existiert
- die Sicherungsdatei nicht dem aktuellen Stand entspricht. Dies trifft zu, wenn zwischen dem Sichern des Systemkerns und dem Auftreten des Systemfehlers der Verschlüsselungsstatus der Festplatte(n) geändert wurde.

Nach Wahl von „Reparieren“ versucht eine Diagnoseroutine den Systemkern zu lokalisieren und wieder zu aktivieren. Dies kann mehrere Minuten dauern. Der Verlauf wird in einer Fortschrittsanzeige dargestellt. Anschließend wird Ihnen mitgeteilt, ob das Reparieren erfolgreich gewesen ist.

ACHTUNG:
Der Versuch, einen Systemfehler mit Reparieren zu beheben, führt nicht immer zum Erfolg. Daher sollten Sie immer eine aktuelle Sicherung des Systemkerns zur Verfügung haben.

27.5.3 Notfalldeinstallation von SafeGuard Easy

Wenn der Systemfehler weder mit „Restaurieren“ noch mit „Reparieren“ zu beheben ist, hilft nur noch das Entschlüsseln der Festplatte samt Ausschalten der Pre-Boot Authentisierung. Nach der Deinstallation wird die Arbeitsstation zweimal automatisch neu gestartet.

Zu diesem Zweck muss jedoch das SafeGuard Easy Benutzerprofil mit entsprechenden Rechten ausgestattet sein. Fehlt einem Benutzer das Recht zur Deinstallation, kann es ihm mit Hilfe des Challenge/Response-Verfahrens erteilt werden.

Zusätzlich sollten Sie nach der Notfallentschlüsselung eine Datenträgerüberprüfung in Windows durchführen. Informationen hierzu finden Sie in Ihrer Windows Dokumentation.

Fehlerhafte Entschlüsselung

Kontaktieren Sie bitte unseren Support, falls die Erstverschlüsselung oder die Entschlüsselung aus irgendeinem Grund fehlschlägt.

Erweiterte Forensic Unterstützung (Parameter /NoReboot)

Die SafeGuard Easy Notfallentschlüsselung bietet für das Notfallprogramm `Sgeasy.exe` den Kommandozeilen-Parameter `/NoReboot`. Mit diesem Kommandozeilenparameter wird der automatische Neustart nach der Notfallentschlüsselung unterdrückt. Dies ist nützlich zur forensischen Analyse der Platte.

Ablauf:

1. Booten Sie das Notfallmedium.
2. Starten Sie `Sgeasy.exe /NoReboot`.
3. Die Notfallentschlüsselung / Deinstallation wird abgeschlossen
4. Der PC wird angehalten und ein Informationstext erscheint. In diesem Zustand wird kein Programmstart oder Benutzereingabe akzeptiert.

Festplatte ist defekt

Bitte beachten Sie: Wenn Sie vermuten, dass Ihre verschlüsselte Festplatte physikalisch beschädigt ist, empfehlen wir, die betreffende Festplatte NICHT per Notfallmedium zu entschlüsseln.

Ein physikalischer Defekt macht sich z.B. so bemerkbar: die Festplatte gibt ratternde oder klickende Geräusche von sich, wird nicht mehr vom BIOS erkannt etc.

Unternehmen Sie in diesem Fall keine weiteren Rettungsversuche auf eigene Faust, sondern wenden Sie sich an Spezialisten. Diese werden versuchen, den Inhalt der korrupten Festplatte auf eine intakte zu überspielen und dort eine Notfallentschlüsselung durchzuführen.

Durch externe Hilfe entstehen weitere Kosten, entscheiden Sie selbst, wie wertvoll die Daten auf der defekten Festplatte für Sie sind.

Weitere Informationen zu diesem Thema erhalten Sie in der Utimaco-Wissensdatenbank http://www.utimaco.de/myutimaco.
Nutzen Sie bitte die Suchfunktion der Wissensdatenbank, um nach Stichworten wie „Data & Recovery“ zu suchen.

27.5.4 Hinweise

- **Ablage des Systemkerns**
  Ist die Windows-Bootpartition nicht auf der ersten Festplatte, wird der SafeGuard Easy Systemkern während der Installation automatisch auf der C: - Partition abgelegt. Diese Partition sollte demzufolge nach der Installation nicht mehr formatiert werden, da sie die wichtigsten Windows Informationen (Systemkern, Treiber, etc.) enthält. Wird dennoch eine Formatierung nach der SafeGuard Easy-Installation durchgeführt, muss das System neu installiert werden.

  Die Systemkernsicherung ist system-spezifisch, d.h. der Systemkern kann nur auf dem PC wiederhergestellt werden, auf dem er gesichert wurde.

  Da Sie im Fall eines Systemdefekts wahrscheinlich nicht auf die Festplatte zugreifen können, sollte der Systemkern samt Notfalldateien immer auf einer Diskette, einem Wechselmedium oder dem Netzlaufwerk abgelegt sein.

- **Spracheinstellung im Notfallprogramm Sgeasy.exe**
  Die Sprache der Benutzeroberfläche des Notfallprogramms bestimmt die Datei Sgeasy.hmf (befindet sich auf der Notfalldiskette). Die verschiedenen Ausgaben der Sprachdatei für Deutsch (Sgeasy07.hmf), Englisch (Sgeasy09.hmf) und Französisch (Sgeasy0C.hmf) sind im SafeGuard Easy-Installationsverzeichnis zu finden. Der Benutzer muss die jeweilige Sprachdatei Sgeasy<09,07,0C>.hmf für die Notfalldiskette in Sgeasy.hmf umbenennen, um die gewünschte Sprache in Sgeasy.exe zu erhalten.

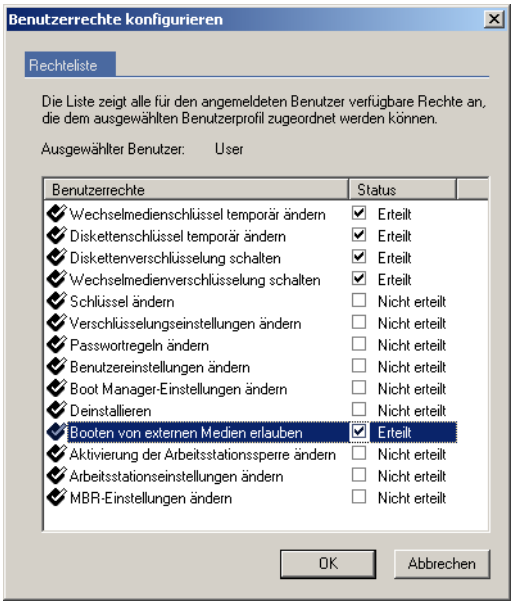
27.6 Nach Booten von externen Medien im Notfall auf verschlüsselte Daten zugreifen

In bestimmten (Notfall-)Situationen wollen Benutzer ein mit SafeGuard Easy verschlüsseltes System von einem externen Medium starten, z.B. um Daten zu retten, wenn das Betriebssystem nicht mehr startet. Benutzer können das System allerdings erst dann von einem externen Bootmedium starten (und auf die PC-Daten zugreifen), nachdem gültige SafeGuard Easy-Zugangsdaten in der Pre-Boot Authentisierung eingetragen wurden.

Als Bootmedien unterstützt SafeGuard Easy MS DOS/Windows 9x Bootdisketten und Boot-CDs/USB-Sticks (für DOS und Windows PE). Wichtig ist, dass die Bootmedien die SafeGuard Easy Treiber enthalten. Die Boot-Methode ist empfehlenswert, um im Notfall Daten zu sichern, bevor das Betriebssystem repariert bzw. SafeGuard Easy per Notfall-Deinstallation entfernt wird.

27.6.1 Voraussetzung

Das Booten von einem externen Medium ist ein administratives SafeGuard Easy-Recht, das in der Grundeinstellung nur dem SafeGuard Easy-Benutzer „SYSTEM“ gewährt ist. Soll das System von einem externen Medium gestartet werden, muss das in der Pre-Boot Authentisierung angemeldete SafeGuard Easy-Profil über das Recht „Booten von externen Medien erlauben“ verfügen.



27.6.2 Vorgehensweise

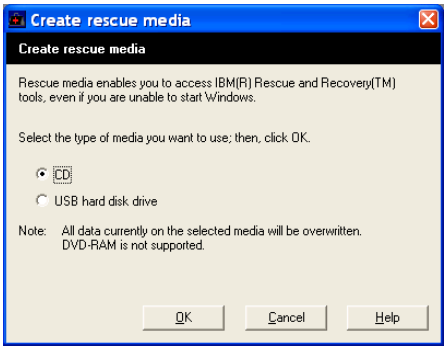
1. PC einschalten und System von der Festplatte booten.
2. Pre-Boot Authentisierung erscheint.
3. SafeGuard Easy-Zugangsdaten in Pre-Boot Authentisierung eingeben.
4. a) **Boot-Diskette** einlegen, Daten mit **[Eingabe]** bestätigen.

   b) **Boot-CD** einlegen, Daten mit **[F7]** bestätigen.
5. Der PC startet neu vom externen Bootmedium.
6. Nach erfolgreichem Neustart ist es möglich, auf Daten zuzugreifen oder diese zu sichern.

27.6.3 Hinweise

- Das erfolgreiche Booten über CD / USB-Stick ist abhängig vom BIOS Support des PC!
- Eine Beschreibung für das Erstellen einer bootfähigen Windows PE CD ist in unserer Wissensdatenbank **http://www.utimaco.de/myutimaco** abgelegt.

  Nutzen Sie bitte die Suchfunktion der Wissensdatenbank, um nach Stichworten wie „BartPE“ oder „SafeGuard Easy“ zu suchen.
- Das Rescue and Recovery Feature „Create Rescue Media“ erstellt bei installiertem SafeGuard Easy automatisch eine CD inkl. SafeGuard Easy Treibern. Die Option ist aufrufbar über Programme / Thinkvantage (Access IBM).


Create rescue media
Create rescue media
Rescue media enables you to access IBM(R) Rescue and Recovery(TM) tools, even if you are unable to start Windows.
Select the type of media you want to use; then, click OK.
CD
USB hard disk drive
Note: All data currently on the selected media will be overwritten. DVD-RAM is not supported.
OK
Cancel
Help

27.6.4 Was tun, wenn...

...das Booten nach der Pre-Boot Authentisierung von einem externen Medium fehlschlägt?
Folgende Gründe sind denkbar:

- Der angemeldete SafeGuard Easy-Benutzer verfügt nicht über das Recht „Booten von externem Medium erlaubt“.
- Die Verschlüsselung der Festplatte wurde angestoßen, ist aber noch nicht beendet.

Für das Fehlschlagen des Bootens von Diskette sind zusätzlich folgende Gründe denkbar:

- Das Diskettenlaufwerk wird im PC nicht über den Standard-Disketten-Controller angesprochen, sondern über die USB-Schnittstelle.
- Das Diskettenlaufwerk ist verschlüsselt, die Bootdiskette ist jedoch nicht verschlüsselt.

28 Systemstatus von SafeGuard Easy anzeigen

SafeGuard Easy besitzt mit SGEState ein Kommandozeilentool, das den aktuellen Status einer SafeGuard Easy-Installation auf einem Benutzer-PC anzeigt (Versionsangabe, Verschlüsselungsmodus, Verschlüsselt/Nicht verschlüsselt etc.). Das Tool eignet sich am besten für Installationen in großen Umgebungen, da ein Administrator auf einfache Weise den Status einer SafeGuard Easy-Installation abfragen kann.

Man kann SGEState aber beispielsweise auch so einsetzen, dass bestimmte Tätigkeiten/Prozesse erst ausgeführt werden, wenn die Installation von SafeGuard Easy (bzw. die Verschlüsselung) abgeschlossen ist.

SGEState ist nach der Installation des SafeGuard Easy Client-Pakets im SafeGuard Easy-Programmverzeichnis zu finden.

28.1 Reporting

SGEState kann auch zu Reporting-Zwecken genutzt werden:

- Der Return Code von SGEState kann serverseitig von Third-Party Management Tools ausgewertet werden.
- SGEState /LD liefert eine für LANDesk (und ggf. andere Produkte) formatierte Ausgabe, die in eine Datei umgeleitet und auf den Server zur Auswertung transportiert werden kann.

28.2 Parameter

SGEState kann mit folgenden Parametern aufgerufen werden:

```
SGESTATE [/?] [/Q | /L | /LD] [/E [/Mvalue]] [/Dvalue] [/R]
```

SGEState /? gibt einen Überblick über alle verfügbaren Kommandozeilenparameter.

```
/Q...Quiet mode: No output, program ends with return code:

  0...SafeGuard Easy not installed.
  2...SafeGuard Easy installed.
  3...SafeGuard Easy installed. Encryption or decryption process active.
255...An error occurred during the check. In this case, a message
      to the console will state the nature of the problem.

/L...Loud mode. Will display details to the console including:

Operating System: [WINDOWS 2000 | WINDOWS XP | WINDOWS SERVER 2003]

Installation Status         : [INSTALLED | NOT INSTALLED | UNKNOWN |
                               INSTALLED (NOT READY FOR BACKUP)]
Version number              : [N/A | number]
Installation Mode           : [N/A | STANDARD | PARTITIONED | BOOT PROTECTION |
                               UNKNOWN]
Disk Encryption             : [N/A | OFF | ON]
Floppy Encryption           : [N/A | OFF | ON]
Removable Media Encryption  : [N/A | OFF | ON]
Initial Encryption          : [N/A | ACTIVE | INACTIVE]

Pre Boot Authentication     : [N/A | OFF | ON]
Current Authentication      : [N/A | USER | WAKE ON LAN]
Secure Auto Logon           : [N/A | OFF | ON]
Secure Smartcard Auto Logon: [N/A | OFF | ON]
SGE Management Server       : [N/A | <UNMANAGED> | OFFLINE | server]

Return code                 : [ReturnCode]

/LD...The details are displayed in LANDesk mode:

/E...Extended return code:

En-/Decryption in process          :  1
SafeGuard Easy installed           :  2
Floppy Encryption "ON"             :  4
Disk Encryption "ON"               :  8
Installation Mode "Boot Protection": 16 (hex 10)
Installation Mode "Partitioned"    : 32 (hex 20)
Installation Mode "Standard"       : 64 (hex 40)
                                     only one mode is possible, (16, 32 or 64)

/Mvalue...value mask for extended return code 1..127

For example: SGESTATE /E produces return code 43 (hex 2b). This indicates:
Partitioned mode, Disk Encryption "ON", SGEasy installed, Encryption in process

For example: SGESTATE /E /M15 produces return code 11 (hex 0b)

/Dvalue...value for desired return code 0..127
          The return code is computed until the desired one is reached
          Calculation can be stopped by pressing any key

/R...the return code is stored in the registry

The input charaters are not case sensitive.
```

29 Protokollierung

Die Aufzeichnung sicherheitsrelevanter Vorfälle ist Voraussetzung für eine gründliche Systemanalyse. Anhand der protokollierten Ereignisse können Vorgänge auf einer Arbeitsstation bzw. innerhalb eines Netzwerks exakter nachvollzogen werden. Durch die Protokollierung können z.B. Schutzverletzungen unautorisierter Dritter nachgewiesen werden. Dem Administrator bietet die Protokollierung auch eine Hilfe, um irrtümlich verwehrte Benutzerrechte ausfindig zu machen und zu korrigieren.

Die Protokollierung zeichnet Ereignisse auf, die installierte SafeGuard-Produkte auslösen. Der Benutzer mit den entsprechenden Rechten kann die protokollierten Ereignisse entweder direkt über die Windows eigene Ereignisanzeige einsehen oder sie für Archivierungszwecke in eine selbstdefinierte Datei exportieren. Protokolliert werden Daten entweder lokal oder per Fernprotokollierung zu einer zentralen Arbeitsstation geschickt.

Zusätzlich zur reinen Protokollierung gibt es einen Filtermechanismus, der hilft, relevante Ereignisse auszuwählen.

Folgende SafeGuard Easy Ereignisse zeichnet die Protokollierung auf:

- Ablauf des Anmeldevorganges an der Pre-Boot Authentisierung (erfolgreich/fehlgeschlagen)
- Administrationstätigkeiten (Erzeugen eines Benutzers etc.)
- Abläufe bei einer zentralen Administration (Client wurde Server zugeordnet etc.)
- Erfolgreiche/fehlgeschlagene Ausführung von Konfigurationsdateien.
- Installations-/Deinstallationsvorgänge
- Ver-/Entschlüsselungsvorgänge

29.1 Anwendungsgebiete

Die Protokollierung ist eine benutzerfreundliche Lösung zum Aufzeichnen von Ereignissen. Beispiele zeigen einige typische Szenarien, wie die Protokollierung eingesetzt werden kann.

Zentrale Überwachung von Arbeitsstationen im Netzwerk

Der Administrator will z.B. regelmäßig über sicherheitskritische SafeGuard-Ereignisse (z.B. Ausführen von Dateien, für die ein Benutzer keine Erlaubnis hat etc.) informiert werden. Er kann die Protokollierung so konfigurieren, dass diese SafeGuard-Ereignisse von bestimmten Computern automatisch an die Ereignisanzeige oder eine selbstgewählte Protokolldatei auf einer definierte Arbeitsstation umgeleitet und gespeichert werden. Die Vorgänge auf verschiedenen Arbeitsstationen werden also kontinuierlich kontrolliert, ohne dass Mitarbeiter Einfluss auf die Aufzeichnungen nehmen können. Um diesen Mechanismus zu nutzen ist der Einsatz der Microsoft Komponente Message Queuing erforderlich.

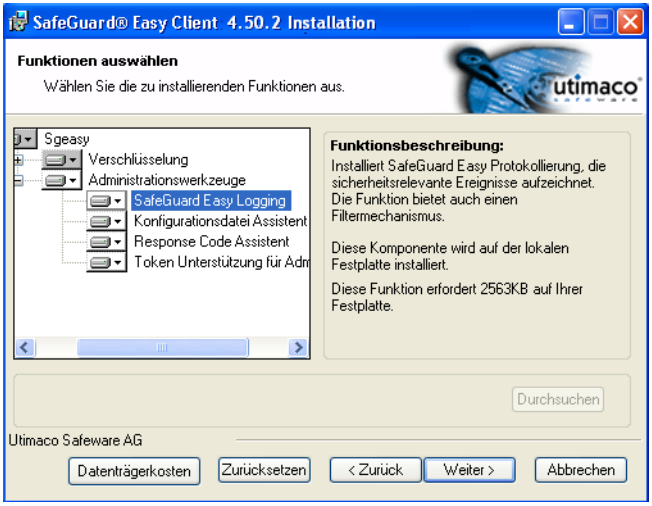
Überwachen mobiler Benutzer

Mobile Benutzer sind in der Regel nicht ständig mit dem Unternehmensnetzwerk verbunden. Ein Außendienstmitarbeiter nimmt z.B. für einen Termin sein Notebook vom Netz. Sobald er sich wieder am Netzwerk anmeldet, werden über die Protokollierung die während der Offline-Zeit protokollierten SafeGuard-Ereignisse übertragen. Die Protokollierung liefert dem Administrator somit einen genauen Überblick über die Benutzeraktivitäten während der betreffende Computer nicht ans Netzwerk angeschlossen war.

29.2 Protokollierung installieren

Um die SafeGuard Easy Protokollierung zu installieren, aktivieren Sie das Feature SafeGuard Logging während der SafeGuard Easy Client Installation.

1. Starten Sie `Sgeasy.msi` im Client-Verzeichnis der Produkt-CD.
2. Wenn der Dialog "Funktionen auswählen" angezeigt wird, aktivieren Sie neben den bereits ausgewählten Funktionen das Modul "SafeGuard Easy Logging". Setzen Sie den Installationsvorgang fort.



3. Starten Sie nach Abschluss der Installation Ihren Computer neu.

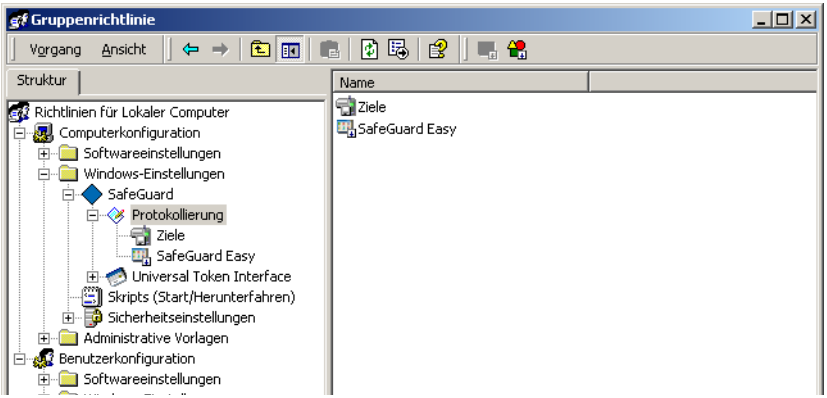
29.3 Protokollierung konfigurieren

Administriert werden alle Einstellungen für die Protokollierung mit Hilfe des Snap-In Gruppenrichtlinie in der Microsoft Management Console (MMC). Die MMC ist in der Grundeinstellung in die Betriebssysteme Windows 2000 und Windows XP integriert.

So rufen Sie das Snap-In Gruppenrichtlinie auf:

1. Klicken Sie auf Start / Ausführen und tippen Sie „mmc“ ein.
2. Die Microsoft Management Console öffnet sich. Öffnen Sie das Menü Konsole, wählen Sie Snap-In hinzufügen/entfernen und klicken Sie auf *Hinzufügen*.
3. Doppelklicken Sie unter *Eigenständiges Snap-In hinzufügen* auf das Snap-In Gruppenrichtlinie.
4. Wählen Sie „Lokaler Computer“ für die lokale Protokollierung oder in einer Active Directory-Umgebung über die [Durchsuchen]-Schaltfläche ein Gruppenrichtlinienobjekt.

Danach wird der Knoten **Protokollierung** unter Computer- und Benutzerkonfiguration im Ordner Windows Einstellungen / SafeGuard angezeigt.



29.4 Ereignisse protokollieren

Für die Protokollierung der Ereignisse müssen nacheinander folgende Schritte durchgeführt werden:

- Ausgabeziel der Ereignisse festlegen
- Ereignisse bestimmen, die aufgezeichnet werden sollen
- Protokollierte Daten anzeigen

29.4.1 Ziel festlegen

Das Fehlschlagen bzw. erfolgreiche Ausführen von Ereignissen wird in sogenannten Ausgabemodulen dokumentiert. Die Protokollierung nennt diese Ausgabemodule *Ziele*. Ziel kann die Windows-eigene Ereignisanzeige oder eine selbstgewählten Protokolldatei sein. Ebenso ist die Protokollierung von Ereignissen einer Arbeitsstation zur anderen möglich. In ein Ziel schreibt die Protokollierung nur die Ereignisse, die mit einem Utimaco-Produkt verknüpft sind.

Ereignisanzeige (EventLog)

Ein Werkzeug für die Protokollierung der Überwachungsinformationen ist die Windows Ereignisanzeige. Die Ereignisanzeige kann Protokolle für System-, Sicherheits- und Anwendungs-Ereignisse anzeigen und verwalten, sowie diese Ereignisprotokolle sichern.

Protokolldatei (LogFile)

Zu Archivierungszwecken können die SafeGuard-Protokolldateien mit verschiedenen Werkzeugen (z.B. MS-Excel) individuell aufbereitet und ausgewertet werden.

Fernprotokollierung (Remote Log)

Aufgabe der Fernprotokollierung ist der Datenaustausch zwischen einer Zielarbeitsstation und einer entfernten Arbeitsstation in einem Netzwerk. Dabei sammelt der Zielrechner in seiner Ereignisanzeige oder einer Protokolldatei Informationen (Ereignisse), die von der entfernten Arbeitsstation per Fernprotokollierung übertragen werden.

Die Fernprotokollierung funktioniert nur in Verbindung mit dem Basismodul von SafeGuard Advanced Security.

HINWEIS:
Für den Austausch von Protokollierungsdaten zwischen mehreren Arbeitsstationen wird empfohlen, den Mechanismus der Fernprotokollierung einzusetzen und das Schreiben in eine Protokolldatei auf einem freigegebenen Netzlaufwerk zu vermeiden.

ACHTUNG:
Bei der Protokollierung auf einen Windows NT Server muss die Fernprotokollierung eingesetzt werden, da der System-Account mit dem die Protokollierung arbeitet, keine Netzwerk-Credentials hat und somit nicht in eine angegebene Protokolldatei schreiben kann.

29.4.2 Neues Ziel erzeugen

So erzeugen Sie ein neues Ziel:

1. Klicken Sie auf Ziele.
2. Klicken Sie auf das Icon oder im Kontextmenü von *Ziele* auf *Neues Ziel hinzufügen*.
3. Der Dialog *Neues Ziel* erscheint.

Name:

Tragen Sie hier eine selbstgewählte Bezeichnung für das Ziel ein. Der Zielname kann aus beliebig vielen Leer- bzw. Sonderzeichen bestehen.

Typ:

Legt den Ort der Ereignisprotokollierung fest

- Wählen Sie *Ereignisanzeige (EventLog)*, wenn die Ereignisse in der Ereignisanzeige abgelegt werden sollten.
- Wählen Sie *Protokolldatei (LogFile)*, wenn die Ereignisse in einer Datei abgespeichert werden sollen.

  HINWEIS: Die gewählte Datei darf nicht schreibgeschützt sein.
- Wählen Sie *Fernprotokoll (RemoteLog)*, wenn die Ereignisse auf einer anderen Arbeitsstation abgelegt werden sollen.
  (Nur verfügbar in Kombination mit dem Basismodul von SafeGuard Advanced Security!)

Ziel:

Wählt über [Suchen] die Protokolldatei bzw. der Arbeitsstation aus zu der die Ereignisse übermittelt werden.

Die Anzahl der anlegbaren Ziele ist unbegrenzt.

29.4.3 Ziel löschen

Benötigen Sie ein Ziel nicht mehr, können Sie dieses aus der Zielliste entfernen.

Klicken Sie mit der rechten Maustaste auf das Ziel, das Sie entfernen wollen. Wählen Sie den Befehl Löschen und bestätigen Sie die Sicherheitsabfrage.

> ***HINWEIS:***
> Sobald ein Ziel gelöscht wird, wird allen damit verbundenen Ereignissen der Status „Deaktiviert“ zugewiesen.

29.4.4 Ziel kopieren

Kopiert werden Ziele zwischen verschiedenen Gruppenrichtlinienobjekten (GPOs)

- über die Kontextmenübefehle Kopieren/Einfügen des Ordners „Ziele”.
- mit Drag&Drop

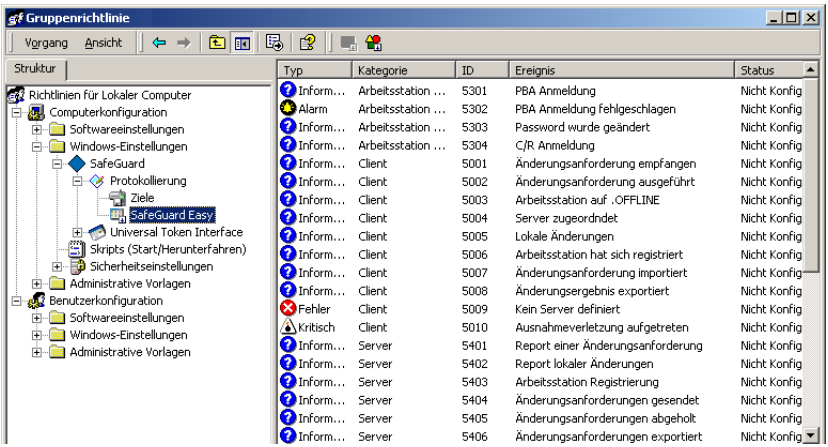
Alle in einer GPO bisher vorhandenen Ziele werden überschrieben!

29.5 Ereignisse auswählen

Jedes Produkt der SafeGuard-Familie reiht unter der Protokollierung verschiedene Ordner ein, die vordefinierte Ereignisse für jedes der installierten Produkte beinhalten.

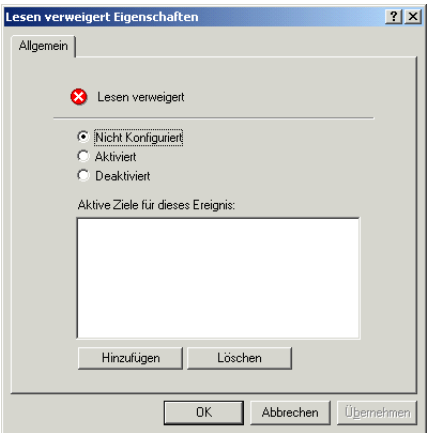
So konfigurieren Sie Ereignisse und ordnen diese definierten Zielen zu:

1. Klicken Sie auf einen der Ordner unter **Protokollierung**.
2. Im rechten Bildschirmfeld erscheinen verschiedene Spalten. Ein Klick auf eine Spaltenüberschrift sortiert die Ereignisse nach Typ, Kategorie etc.


Gruppenrichtlinie
Vorgang
Ansicht
Struktur
Richtlinien für Lokaler Computer
Computerkonfiguration
Softwareeinstellungen
Windows-Einstellungen
SafeGuard
Protokollierung
Ziele
SafeGuard Easy
Universal Token Interface
Skripts (Start/Herunterfahren)
Sicherheitseinstellungen
Administrative Vorlagen
Benutzerkonfiguration
Softwareeinstellungen
Windows-Einstellungen
Administrative Vorlagen
Typ Kategorie ID Ereignis Status
Inform... Arbeitsstation ... 5301 PBA Anmeldung Nicht Konfig
Alarm Arbeitsstation ... 5302 PBA Anmeldung fehlgeschlagen Nicht Konfig
Inform... Arbeitsstation ... 5303 Password wurde geändert Nicht Konfig
Inform... Arbeitsstation ... 5304 C/R Anmeldung Nicht Konfig
Inform... Client 5001 Änderungsanforderung empfangen Nicht Konfig
Inform... Client 5002 Änderungsanforderung ausgeführt Nicht Konfig
Inform... Client 5003 Arbeitsstation auf .OFFLINE Nicht Konfig
Inform... Client 5004 Server zugeordndet Nicht Konfig
Inform... Client 5005 Lokale Änderungen Nicht Konfig
Inform... Client 5006 Arbeitsstation hat sich registriert Nicht Konfig
Inform... Client 5007 Änderungsanforderung importiert Nicht Konfig
Inform... Client 5008 Änderungsergebnis exportiert Nicht Konfig
Fehler Client 5009 Kein Server definiert Nicht Konfig
Kritisch Client 5010 Ausnahmeverletzung aufgetreten Nicht Konfig
Inform... Server 5401 Report einer Änderungsanforderung Nicht Konfig
Inform... Server 5402 Report lokaler Änderungen Nicht Konfig
Inform... Server 5403 Arbeitsstation Registrierung Nicht Konfig
Inform... Server 5404 Änderungsanforderungen gesendet Nicht Konfig
Inform... Server 5405 Änderungsanforderungen abgeholt Nicht Konfig
Inform... Server 5406 Änderungsanforderungen exportiert Nicht Konfig

3. Doppelklicken Sie im rechten Feld auf ein Ereignis oder wählen Sie in dessen Kontextmenü Eigenschaften.

4. Der Eigenschaften-Dialog des Ereignisses erscheint.



In diesem Dialog legen Sie Status und Ausgabeziel fest.

- **Nicht konfiguriert (Standard)**
  Das Ereignis gilt als deaktiviert.

  ACHTUNG:
  Bereits zugewiesene Ziele zu Ereignissen haben Vorrang gegenüber dieser Einstellung. Ist ein Ziel bereits einem Ereignis zugewiesen, ist diese Option hinfällig.

- **Aktiviert:**
  Das Ereignis wird für ein oder mehrere Ziele protokolliert.

- **Deaktiviert:**
  Das Ereignis wird deaktiviert und nicht protokolliert.

Über **[Hinzufügen]** öffnet sich ein Dialog, in dem alle registrierten Ziele angezeigt werden. Die dort markierten Ziele werden in das Feld **Aktive Ziele für das Ereignis** übernommen. **[Löschen]** entfernt aktive Ziele.

5. Klicken Sie [Übernehmen] und dann [OK].

Mehrfachselektion

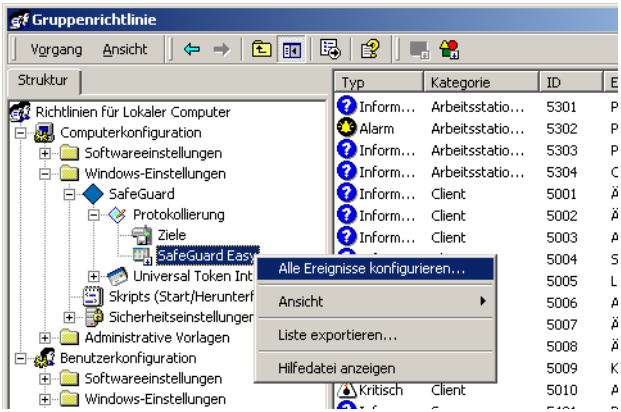
Es können auch mehreren Ereignisse/Ziele ausgewählt werden. Dies geschieht mit Hilfe der Mehrfachselektion.

Wählen Sie über die gewohnten Windows-Mechanismen [Strg]- und [Umschalt]-Taste mehrere Ereignisse aus. Im Kontextmenü gehen Sie auf *Eigenschaften* und geben Status und Ziel an (siehe Abbildung auf Seite 402). Nach einem Klick auf [OK] werden die getroffenen Einstellungen auf alle selektierten Ereignisse angewandt.

29.5.1 Alle Ereignisse konfigurieren

Über den Befehl **Alle Ereignisse konfigurieren** werden in einem Arbeitsschritt Ereignisse mit identischen Einstellungen konfiguriert.

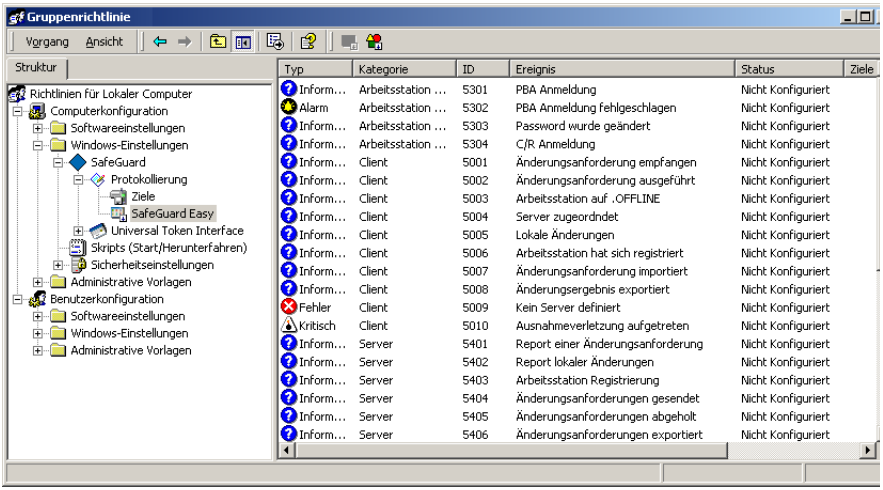
Klicken Sie auf den Ordner Protokollierung oder einen Unterordner (z.B. SafeGuard Easy).



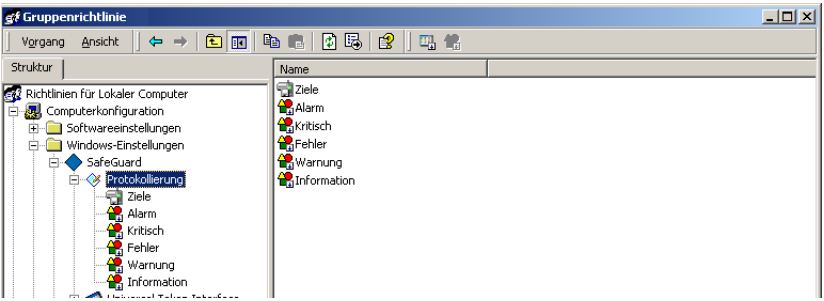
Wählen Sie im Kontextmenü den Befehl „Alle Ereignisse konfigurieren”. Legen Sie im Dialog Alle Ereignisse Eigenschaften Status und aktive Ziele fest. Klicken Sie auf [Bestätigen] und dann auf [OK], gelten für alle Ereignisse die gewählten Einstellungen.

29.5.2 Ansicht ändern

In der Grundeinstellung werden Ereignisse geordnet nach SafeGuard-Applikationen angezeigt.


Gruppenrichtlinie
Vorgang Ansicht
Struktur
Richtlinien für Lokaler Computer
Computerkonfiguration
Softwareeinstellungen
Windows-Einstellungen
SafeGuard
Protokollierung
Ziele
SafeGuard Easy
Universal Token Interface
Skripts (Start/Herunterfahren)
Sicherheitseinstellungen
Administrative Vorlagen
Benutzerkonfiguration
Softwareeinstellungen
Windows-Einstellungen
Administrative Vorlagen
Typ Kategorie ID Ereignis Status Ziele
Inform... Arbeitsstation ... 5301 PBA Anmeldung Nicht Konfiguriert
Alarm Arbeitsstation ... 5302 PBA Anmeldung fehlgeschlagen Nicht Konfiguriert
Inform... Arbeitsstation ... 5303 Password wurde geändert Nicht Konfiguriert
Inform... Arbeitsstation ... 5304 C/R Anmeldung Nicht Konfiguriert
Inform... Client 5001 Änderungsanforderung empfangen Nicht Konfiguriert
Inform... Client 5002 Änderungsanforderung ausgeführt Nicht Konfiguriert
Inform... Client 5003 Arbeitsstation auf .OFFLINE Nicht Konfiguriert
Inform... Client 5004 Server zugeordndet Nicht Konfiguriert
Inform... Client 5005 Lokale Änderungen Nicht Konfiguriert
Inform... Client 5006 Arbeitsstation hat sich registriert Nicht Konfiguriert
Inform... Client 5007 Änderungsanforderung importiert Nicht Konfiguriert
Inform... Client 5008 Änderungsergebnis exportiert Nicht Konfiguriert
Fehler Client 5009 Kein Server definiert Nicht Konfiguriert
Kritisch Client 5010 Ausnahmeverletzung aufgetreten Nicht Konfiguriert
Inform... Server 5401 Report einer Änderungsanforderung Nicht Konfiguriert
Inform... Server 5402 Report lokaler Änderungen Nicht Konfiguriert
Inform... Server 5403 Arbeitsstation Registrierung Nicht Konfiguriert
Inform... Server 5404 Änderungsanforderungen gesendet Nicht Konfiguriert
Inform... Server 5405 Änderungsanforderungen abgeholt Nicht Konfiguriert
Inform... Server 5406 Änderungsanforderungen exportiert Nicht Konfiguriert

Über den Filtermechanismus ist es möglich, Ereignisse sortiert nach Warnstufe anzuzeigen, unabhängig von der Anwendung durch die sie ausgelöst werden (z.B. alle kritischen Ereignisse).



Sie wechseln die Ansichten über die Icons und .

29.6 Protokollierte Ereignisse ansehen

Protokollierte Ereignisse können in der Ereignisanzeige oder der Protokolldatei eingesehen werden.

Dargestellt werden

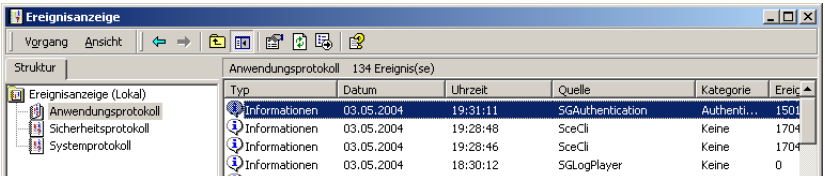
- Computer: Name des Computers, auf dem das protokollierte Ereignis auftrat.
- Datum: Systemdatum, an dem das Ereignis erzeugt wurde.
- Zeit: Systemzeit, an dem das Ereignis erzeugt wurde.
- Benutzer: Benutzer, der beim Auftreten des Ereignisses angemeldet war
- Typ: Klassifizierung des Ereignisses durch Windows, z.B Warnung, Fehler.
- Ereignis-ID: Nummer zur Identifizierung des Ereignisses.
- Quelle: Die Software, die das Ereignis produziert hat.
- Kategorie: Klassifizierung des Ereignisses durch die Quelle.

Die Ereignisse werden immer in der eingestellten Systemsprache ausgegeben.

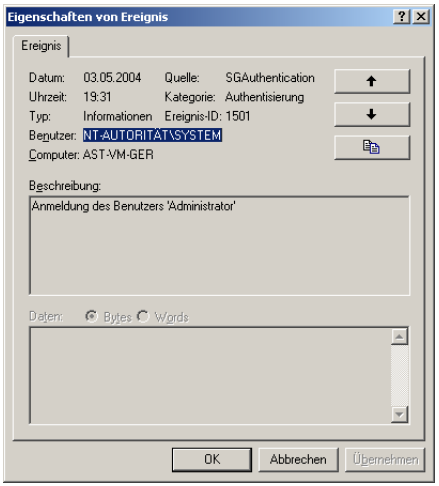
29.6.1 Ereignisanzeige (Event Log)

Angezeigt werden die von der Protokollierung aufgezeichneten Ereignisse im *Anwendungsprotokoll* der Windows-*Ereignisanzeige*.

Zum Starten der Ereignisanszeige klicken Sie unter Windows auf Start, zeigen auf Programme, dann auf Verwaltung und klicken dann auf Ereignisanzeige. Rufen Sie dann das Anwendungsprotokoll auf, werden im sogenannten Detailbereich die protokollierten Ereignisse angezeigt.



Doppelklicken Sie auf ein bestimmtes Ereignis im Detailbereich, erscheinen die Detailinformationen zum Ereignis.



HINWEIS:
Bei der Fernprotokollierung werden in der Ereignisanzeige in den Feldern Computername, Zeit und Datum immer die Daten der Arbeitsstation eingetragen, die die Ereignisse protokolliert. Die Daten des Computers, der ein Ereignis auslöst, erscheint im Feld Beschreibung.

Die Ereignisanzeige von Windows zeigt nicht alle Warnstufen von der Protokollierung an. Deswegen werden die unterschiedlichen Warnstufen in der Ereignisanzeige folgendermaßen ausgegeben:

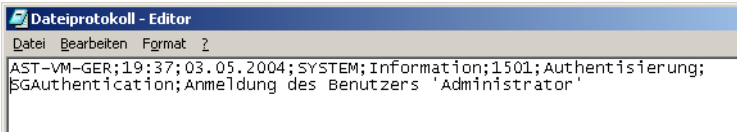
SafeGuard Protokollierung	**Ereignisanzeige**
Notfall Alarm Fehler Kritisch	Fehler
Warnung	Warnung
Notiz	Kein
Information	Information

29.6.2 Protokolldatei (Log File)

Die Protokolldatei(en) der Protokollierung sind das Pendant zur Windows-Protokolldatei. In ihnen werden allerdings nur die Ereignisse abgelegt, die von einem SafeGuard-Produkt ausgelöst wurden. Die Darstellung der Ereignisse erfolgt mittels chronologischem Listing. Sie können die Protokolldaten durch "Speichern unter..." für den Import z.B. in ein Datenbankprogramm bereitstellen, um sie dann ggf. zu konvertieren und auszuwerten.

> ***HINWEIS:***
> Bitte verwenden Sie zum Protokollieren von Ereignissen keine Dateien, die mit EFS verschlüsselt sind oder in einem mit EFS verschlüsselten Ordner liegen.

Der Eintrag in eine Protokolldatei kann beispielsweise so aussehen:



Die einzelnen Einträge haben folgende Bedeutungen:

AST-VM-GER	Computername
19:37	Uhrzeit
03.05.2004	Datum
System	Benutzer oder Gruppe, der/die das Ereignis erzeugt hat.
Information	Warnstufe
1511	Ereignis-ID
Authentisierung	Kategorie
SGAuthentication	Quelle

Anmeldung des Benutzers 'Administrator'	Beschreibung

29.7 Hinweise

- Definiert man als Ausgabeziel eine Protokolldatei auf einem externen Medium, wie z.B. einem Wechselmedium, wird beim Überschreiten dessen Speicherkapazität eine Fehlermeldung in die Ereignisanzeige ausgegeben.
  Utimaco empfiehlt, das Protokollieren in externe Medien soweit wie möglich zu vermeiden, da es u.U. zur Systemverlangsamung führen kann.

- Ereignisse, die nicht in eine Protokolldatei geschrieben werden können, werden als Fehler in die Ereignisanzeige eingetragen.

- Schreiben mehrere Arbeitsstationen per Definition in eine Protokolldatei (z.B. eine Datei auf einem Netzlaufwerk), ergeben sich u.U. bei gleichzeitigem Zugriff der verschiedenen Rechner Überschneidungen. Um in diesem Fall Datenverluste zu vermeiden, löst die Protokollierung diese Konkurrenzsituation folgendermaßen: Sobald auf die definierte Protokolldatei nicht zugegriffen werden kann, da sie in diesem Moment von einer anderen Arbeitsstation in Bearbeitung ist, erzeugt die Protokollierung für die „abgewiesenen“ Arbeitsstationen neue Protokolldateien. Angelegt werden neue Protokolldateien nach folgendem Prinzip:

  Zugriff auf die definierte Standardprotokolldatei Sglog.txt wird verweigert. Die Protokollierung legt die Ersatzdatei Sglog.txt.1 an

  Zugriff auf Protokolldateien Sglog.txt und Sglog.txt.1 wird verweigert. Die Protokollierung legt die Ersatzdatei Sglog.txt.2 an. etc.

Es können maximal 999 Dateien angelegt werden. Bei Überschreiten dieser Zahl werden die Ereignisse automatisch in die Ereignisanzeige geschrieben. Wenn die Protokolldatei die Eigenschaft „Nur Lesen“ besitzt oder ihre Größe 2 GB überschreiten würde, legt SafeGuard Easy eine neue Protokolldatei an. Die durch SGE angelegte Protokolldatei muss bei einer Deinstallation explizit gelöscht werden.

Utimaco empfiehlt das direkte Protokollieren mehrerer Arbeitsstationen in eine Protokolldatei zu vermeiden und für die zentrale Protokollierung der Ereignisse mehrerer Arbeitsstationen generell die Fernprotokollierung einzusetzen.

- **SNMP Traps**
  Sie haben die Möglichkeit SNMP Traps aus der Protokollierung für den Fall zu erzeugen, dass auf einer Clientmaschine ein Ereignis auftritt, das an den Administrator gemeldet werden muss.

  Weitere Informationen zu diesem Thema finden Sie in der Utimaco-Wissensdatenbank **http://www.utimaco.de/myutimaco**.

  Nutzen Sie bitte die Suchfunktion der Wissensdatenbank, um nach Stichworten wie „SNMP“ zu suchen.

30 Zentrale Administration

In Ergänzung zu den bekannten Verwaltungsmechanismen gibt es nun eine eigene Applikation, die zentrale Aufgaben ausführt. Diese verwaltet alle installierten SafeGuard Easy Clients in einem Firmennetzwerk und übernimmt auch die gesicherte zentrale Verteilung etwaiger Konfigurations-Updates an Gruppen von Clients, die Anzeige von deren aktuellem Status, sowie das zentrale Archivieren von Systemkernsicherungen. Auch Clients, die sich nur unregelmäßig mit dem Netzwerk verbinden (Offline-Clients) sind in die zentrale Verwaltung integrierbar.

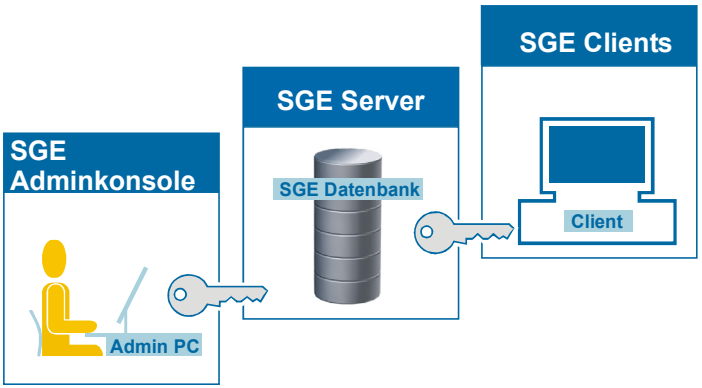
Der aus früheren Versionen bekannte Administrationsmechanismus über Konfigurationsdatei und Softwareverteilungswerkzeug eines Drittherstellers ist weiterhin einsetzbar.

30.1 Funktionsweise

Im Rahmen der zentralen Administration werden SafeGuard Easy Client-PCs von zentraler Stelle über eine Administrationskonsole gesteuert. Die Administrationskonsole verwaltet eine zentrale Datenbank, die die Konfigurationseinstellungen der SafeGuard Easy Clients beinhaltet. Darüber hinaus werden zusätzliche Daten wie z.B. gewünschte Änderungen an Konfigurationseinstellungen ebenfalls in der Datenbank abgespeichert.

Die zentrale Administration von SafeGuard Easy benötigt folgende Komponenten:

- Den SafeGuard Easy Server (im folgenden SafeGuard Easy Server genannt) mit der SafeGuard Easy Datenbank (SafeGuard Easy Datenbank).
- Die SafeGuard Easy Administrationskonsole, die die Datenbank auf dem Server kontrolliert (SafeGuard Easy Administrationskonsole).
- SafeGuard Easy Client PCs (SafeGuard Easy Clients)



Verschlüsselte Kommunikation

Die zentrale SafeGuard Easy Datenbank sammelt verschiedene Informationen über die SafeGuard Easy Clients. Der SafeGuard Easy Administrator nutzt die Administrationskonsole, um die Datenbankinhalte zu steuern und Änderungswünsche in Form von sogenannten „Requests“ zu erstellen. Die SafeGuard Easy Clients lesen mit Hilfe eines Netzwerkagenten die Konfigurationsänderungen über den Server aus der Datenbank und berichten erfolgreiche Änderungen an den Server, der bei erfolgreicher Änderung die neuen Konfigurationseinstellungen in der Datenbank abspeichert. Die Kommunikation mit dem SafeGuard Easy Server übernimmt der SafeGuard Easy Server-Prozess, der ein ODBC Interface nutzt.

30.1.1 SafeGuard Easy Server/SafeGuard Easy Datenbank

Der SafeGuard Easy Server ist die zentrale Anlaufstelle für alle Clients, da hier die Einstellungen aller SafeGuard Easy Clients in einer Datenbank gespeichert werden.

In der Grundeinstellung hat SafeGuard Easy Microsoft Access als Datenbanktyp implementiert, unterstützt jedoch auch den Microsoft SQL Server.

Die SafeGuard Easy Datenbank auf dem SafeGuard Easy Server enthält folgende Informationen über die SafeGuard Easy Clients:

- Aktuelle SafeGuard Easy Einstellungen (ohne Passwörter und Schlüssel)
- Netzwerkname

Diese Informationen sind über die SafeGuard Easy Administrationskonsole einsehbar.

Auf dem Server wird zusätzlich das Verzeichnis Backups erstellt, in dem automatisch von jeder am Server registrierten Arbeitsstation eine Systemkernsicherung erstellt wird, die nach Konfigurationsänderungen aktualisiert wird.

HINWEIS:
Wenn Sie SafeGuard Easy in Verbindung mit der serverbasierten Administration in einer neuen Installation anwenden möchten, so kann sich der Einsatz des Utimaco-Produkts der nächsten Generation - SafeGuard Enterprise - von Anfang an als vorteilhaft für Sie erweisen. SafeGuard Enterprise bietet erweiterte Verwaltungsoptionen, u. a. die Integration von Active Directory, die auf Web Service basierte Verteilung von Richtlinien sowie die Unterstützung von Windows Vista. Weitere Informationen erhalten Sie von Ihrem SafeGuard Easy Vertriebspartner.

HINWEIS:

Im Netzwerk kann es natürlich aus technischen oder organisatorischen Gründen mehrere SafeGuard Easy Server geben, denen die SafeGuard Easy Clients zugeordnet werden können. SafeGuard Easy 4.50 unterstützt **keine Synchronisationsmechanismen** zwischen Servern. Geliefert wird diese Funktionalität u.U. von einer Datenbank mit Replikationsmechanismen.

30.1.2 SafeGuard Easy Administrationskonsole

Die Administrationskonsole ist ein Programm, das auf die Server-Datenbank zugreift und z.B. die zentrale Verteilung von Konfigurationsdateien anstößt. Der Zugriff auf die Administrationskonsole ist nur privilegierten Benutzern erlaubt.

Typische Aufgaben, die die Administrationskonsole übernimmt:

- die Einstellungen von SafeGuard Easy Clients abfragen und ihren Status (Offline, Standard, Push) festlegen.
- die SafeGuard Easy Clients in Gruppen zusammenfassen, um die Administration zu vereinfachen.
- neue Konfigurationen erzeugen, die an die SafeGuard Easy Clients verteilt werden.
- das korrekte Abarbeiten der verteilten Konfigurationsdateien überwachen

Die Administrationskonsole muss nicht notwendigerweise auf der gleichen Maschine wie der SafeGuard Easy Server laufen, sondern kann auf jedem Rechner im Netzwerk installiert und aufgerufen werden, es muss nur der Name des SafeGuard Easy Server-Rechners bekannt sein und eine Netzwerkverbindung bestehen.

Es ist zur Wahrung der Datenkonsistenz **nur eine administrative Verbindung** zur selben Zeit möglich. Der Versuch, mehrere Verbindungen aufzubauen, schlägt fehl.

30.1.3 SafeGuard Easy Clients

SafeGuard Easy Clients sind mit installierter „Server Anbindung“ in der Lage, mit dem SafeGuard Easy Server eine Verbindung aufzubauen. Die Verbindung zwischen SafeGuard Easy Server und SafeGuard Easy Client ermöglicht ein Netzwerkagent und der UNC NETBIOS Name des SafeGuard Easy Servers, die den Clients bei der Installation mitgegeben werden.

Der SafeGuard Easy Client berichtet bei der Erstregistrierung am SafeGuard Easy Server

- seine SafeGuard Easy-Konfigurationseinstellungen
- die GUID
- seinen öffentlichen Schlüssel
- seinen Netzwerknamen.

Darüber hinaus erfolgt bei der Erstregistrierung auch der Austausch des öffentlichen Schlüssel des Servers.

Bei jeder weiteren Kontaktaufnahme mit dem Server fragt der SafeGuard Easy Client nach einer Aktualisierung der für ihn relevanten Einstellungen. In der Regel versuchen die SafeGuard Easy Clients mit dem SafeGuard Easy Server jedesmal eine Verbindung aufzunehmen, wenn der PC bootet. Während dieser Phase werden alle Änderungen, die zentral auf dem SafeGuard Easy Server lagern, abgeholt und auf dem Client ausgeführt.

Änderungen, die lokal am SafeGuard Easy Client vorgenommen werden (wenn z.B. der Administrator vor Ort Einstellungen vornimmt), berichtet der Client sofort an den Server, um die Datenbank auf dem aktuellsten Stand zu halten. Im Fall einer Deinstallation meldet der Client diese Deinstallation an den Server, welcher den Eintrag für den betreffenden Client aus der Datenbank löscht.

30.1.4 Unterstützte SafeGuard Easy Client-/ SafeGuard Easy Server-Kombinationen

SafeGuard Easy Client und SafeGuard Easy Server-Versionen sind grundsätzlich beliebig miteinander kombinierbar, z. B. arbeiten SafeGuard Easy Server V4.50 problemlos mit SafeGuard Easy Clients V4.40 und umgekehrt.

Für SafeGuard Easy Clients < V4.11 gelten allerdings folgende Einschränkungen in der Funktionalität:

- keine Änderung des Client Status nach .OFFLINE
- keine Neuregistrierung eines Clients
- keine Umregistrierung eines Clients

30.2 Datenaustausch zwischen Client und Server

Im Rahmen der zentralen Administration werden sensible SafeGuard Easy Informationen nicht mehr nur per Konfigurationsdateien übermittelt, sondern online zwischen SafeGuard Easy Server und SafeGuard Easy Client ausgetauscht. Diese Verbindung muss geschützt und konfiguriert werden.

30.2.1 Sichere Kommunikation

Um die SafeGuard Easy Informationen adäquat zu schützen, ist die Datenübermittlung verschlüsselt. Verschlüsselung der Verbindung macht aber nur Sinn, nachdem sich jeder Client für den Informationsaustausch am SafeGuard Easy Server authentisiert hat und umgekehrt.

HINWEIS:
Client und Server kommunizieren über den RPC/DCOM Dienst von Microsoft. Es kann frei definiert werden, über welchen Port bzw. welches Protokoll die Kommunikation ablaufen soll.
Wenn Sie eine Firewall einsetzen, müssen Sie die Ports an ihrer Firewall freischalten, über die Client und Server kommunizieren sollen.

Authentisierung Client / Server

SafeGuard Easy verwendet zur beidseitigen Authentisierung eine starke Verschlüsselung mit Public/Private Key-Verfahren. Zur Erzeugung des Schlüsselpaars wird das RSA-Verfahren eingesetzt und eine Schlüssellänge von 1024 bit verwendet. Die Kommunikation zwischen Client und Server wird durch das Interlock-Protokoll geschützt.

Wenn noch kein RSA Schlüsselpaar vorhanden ist, wird dies während der Installation der SafeGuard Easy Software auf Client und Server erzeugt. Einmal erzeugt, bleibt das Schlüsselpaar unverändert bestehen. Wenn beide Parteien zum allerersten Mal in Kontakt treten, werden die öffentlichen Schlüssel ausgetauscht. Sowohl Client als auch Server speichern den öffentlichen Schlüssel und „kennen“ sich von diesem Zeitpunkt an.

Optional kann die Erzeugung des Schlüsselpaars auch von einem Trusted Platform Module wie dem Lenovo ESS Chip übernommen werden. Dies garantiert zusätzliche Hardware-Sicherheit für den Schlüsselspeicher, ist allerdings langsamer als die reine Software-Lösung.

Verschlüsselung der Daten während des Transfers

Alle SafeGuard Easy-Informationen, die vom und zum SafeGuard Easy Server übertragen werden, sind verschlüsselt. Nach erfolgreicher beidseitiger Maschinenauthentisierung wird ein zufälliger symmetrischer Session Key erzeugt, ausgetauscht und für den verschlüsselten Datentransfer in der Zeit der Verbindung genutzt.

Für jede neue Verbindung zwischen SafeGuard Easy Client-Maschine und SafeGuard Easy Server wird ein neuer Session Key erzeugt. Das gleiche Verfahren gilt auch für die Kommunikation zwischen SafeGuard Easy AdminKonsole und SafeGuard Easy Server.

Für die Verschlüsselung des Session Keys wird RC4 mit einem 128 bit Schlüssel verwendet. Der Session Key kann vom Client oder vom Server erzeugt werden und wird mit dem öffentlichen Schlüssel des Empfängers verschlüsselt bevor er gesendet wird.

30.2.2 Zu erwartende Netzlast

Ob nun Konfigurationsupdates beim Hochfahren des SafeGuard Easy Clients abgefragt werden oder nach einem definierten Zeitraum: Die Menge der Daten unterscheidet sich nur geringfügig und zwar in Abhängigkeit davon, ob bzw. welche Änderungen es gibt. In beiden Fällen werden Daten ausgetauscht, deren Größe im Bereich um 2 KB liegt. Die exakte Größe hängt ein wenig davon ab, wie viele Änderungen enthalten sind.

Wenn Sie bereits Konfigurationsdateien für die Installation/Konfiguration von SafeGuard Easy nutzen, gibt deren Dateigröße eine ungefähre Vorstellung von der Datenmenge.

Aufgrund der unter Intervall für Datenaustausch zwischen Client und Server definieren' beschriebenen Konfigurierbarkeit des Datenaustausch-Intervalls trägt die zentrale SafeGuard Easy Administration aus Utimaco-Sicht nur unwesentlich zu höherer Netzwerklast bei.

30.2.3 Intervall für Datenaustausch zwischen Client und Server definieren

Generell stellt ein SafeGuard Easy Client regelmäßig beim Hochfahren beim SafeGuard Easy Server eine Anfrage, ob Änderungen durchzuführen sind. Weitere Anfragen finden nach definierten zeitlichen Abständen statt. Der **Standard-Wert** für weitere Aktualisierungsanfragen ist auf **6 Stunden** eingestellt.

Dieses Intervall kann mit standardmäßigen Windows-Mechanismen zentral angepasst werden, denn es handelt sich dabei um einen Registry-Eintrag.

Zum Anpassen des Intervalls erzeugen Sie also folgenden Registry Key [DWORD-Wert] neu:

HKEY_LOCAL_MACHINE
SOFTWARE
Utimaco
SGEasy

„**NotifyPeriod**“=<Intervall>

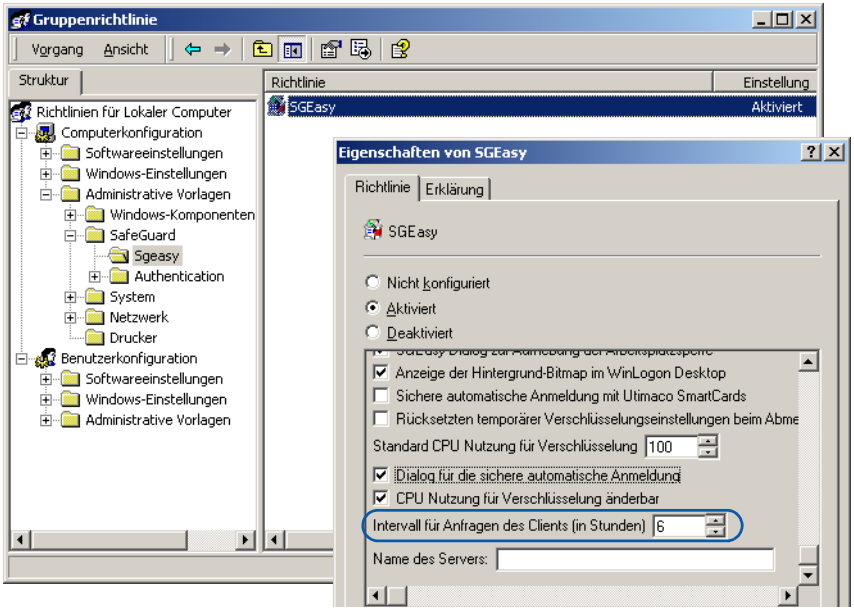
Wenn ein Wert vorhanden ist, fragen Clients im angegebenen Intervall nach Requests (mögliche Werte: 1 bis X Stunden).

Das Intervall ist auch über eine Richtlinie in Utimacos administrativer Vorlage bestimmbar (siehe ’Häufig verwendete Registry-Einstellungen für SafeGuard Easy über die administrative Vorlage ändern’).

Die Richtlinie ist zu finden unter

Computerkonfiguration
\Administrative Vorlagen
\SafeGuard
\Sgeasy

Auf der Eigenschaftenseite von „SGEasy“ ist unter „Intervall für Anfragen an den Server (in Stunden)“ der gewünschte Wert einzutragen.



30.3 Installation

Hinweis zu Windows XP SP 2/ Windows Server 2003 SP1:
Bei Verwendung des optionalen zentralen Administrationsservers bzw. der Remote Administration von SafeGuard Easy 4.x sind besondere Konfigurationseinstellungen in Windows XP SP2 und Windows Server 2003 SP 1zu treffen.

Alle nötigen Einstellungen sind in unserer Wissensdatenbank http://www.utimaco.de/myutimaco im **Knowledge Item „106898 SafeGuard Easy and SP2 Configuration for Windows XP“** beschrieben. Nutzen Sie die Suchfunktion, und geben Sie die Nummer „**106898**“ ein.

Zusätzlich ist auf der CD im Verzeichnis \Tools\DCOM eine Applikation vorhanden, mit der man die Konfigurationseinstellungen automatisch setzen kann, um die zentrale Administration und die Remote Administration zu nutzen.

Vorbereitung

- **High Encryption Package installieren**

  Voraussetzung für die zentrale Administration ist, dass die Betriebssysteme auf Client, Server und dem PC mit der Administrationskonsole die Verschlüsselung mit 128 bit Schlüsseln unterstützen. Dazu muss überall das „High Encryption Package“ von Microsoft installiert sein. Ob dies auf einem PC der Fall ist, erfährt man u.a. über den Internet Explorer (Menü Hilfe / Info / Verschlüsselungsstärke).

  Das High Encryption Package ist bei Windows XP standardmäßig installiert, bei Windows 2000 ab dem Service Pack 2.

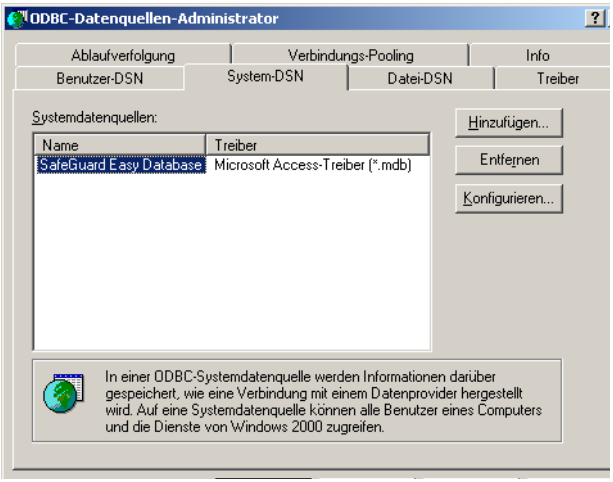
- **Ports**
  Client und Server kommunizieren über den RPC/DCOM Dienst von Microsoft. Es kann frei definiert werden, über welchen Port bzw. welches Protokoll die Kommunikation ablaufen soll.
  Wenn Sie eine Firewall einsetzen, müssen Sie die Ports an ihrer Firewall freischalten, über die Client und Server kommunizieren sollen.

30.3.1 SafeGuard Easy Server/Datenbank installieren

Der Rechner, der die SafeGuard Easy Datenbank hält, ist das „Kernstück“ der zentralen Administration und sollte als erstes eingerichtet werden bzw. es sollte zumindest der Rechnername bekannt sein, um ihn an die SafeGuard Easy Clients weitergeben zu können.

Der SafeGuard Easy Server kann sich auf einem physikalischen Netzwerkserver oder auf einer beliebigen Arbeitsstation im Netz befinden. Voraussetzung für die Anbindung eines Clients an die zentrale SafeGuard Easy Datenbank ist, dass ein entsprechendes Netzwerkprotokoll auf allen Arbeitsstationen installiert und aktiv ist.

Mit Installation der Server-Komponente wird keine Anwendung installiert, sondern nur eine Microsoft Access Datenbank im SafeGuard Easy-Installationsverzeichnis (Sgeasy.mdb) des Servers erzeugt (siehe Systemsteuerung / Verwaltung / Datenquellen (ODBC)). Diese Datenbank ist passwortgeschützt.

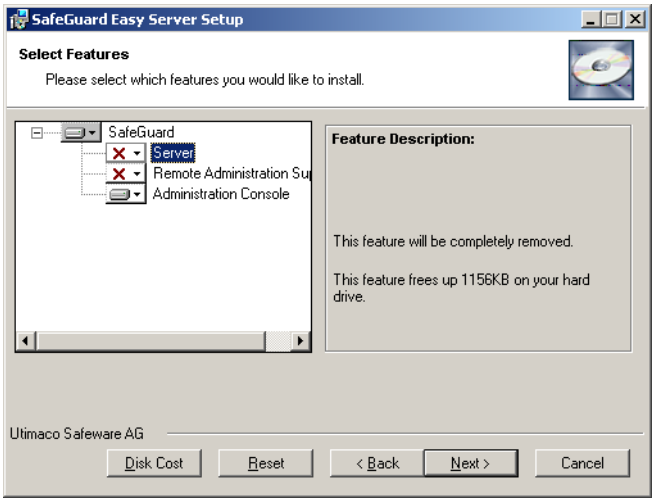


Installieren Sie den SafeGuard Easy Server durch Aufrufen von `Server.msi` aus dem CD-Verzeichnis \SERVER. Wählen Sie im Rahmen einer „Angepassten“ Installation die Option „Server“ aus. Sobald Sie fertig sind, müssen Sie ihr System neu starten.

30.3.2 SafeGuard Easy Administrationskonsole installieren

Da es meistens unerwünscht ist, direkt auf dem Server Installationen und Konfigurationen durchzuführen, sollte die Datenbank von einer administrativen Workstation aus administriert werden. Sie können eine beliebige Arbeitsstation zur administrativen Arbeitsstation machen, es muss nur eine Netzwerkverbindung zu der Server-Maschine bestehen.

Installieren Sie die Administrationskonsole durch Aufrufen von `Server.msi` aus dem CD-Verzeichnis \SERVER. Wählen Sie im Rahmen einer „Angepassten“ Installation die Option „Administrationskonsole“ aus und setzen Sie die Installation fort.



Sobald Sie fertig sind, müssen Sie ihr System neu starten.

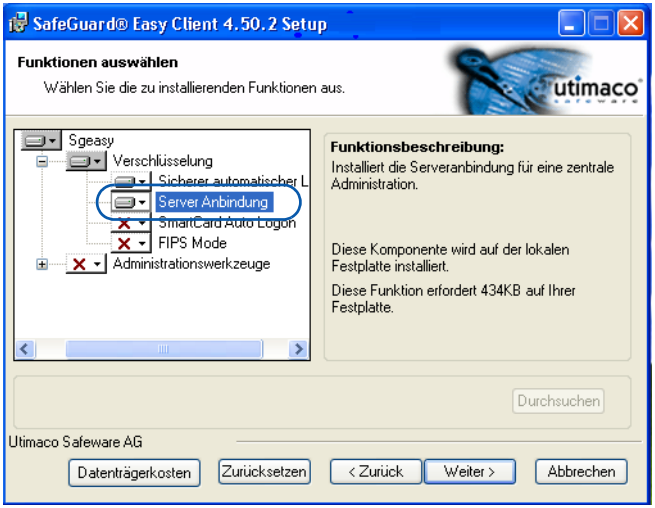
Nach dem Neustart finden Sie unter Programme / Utimaco / SafeGuard Easy die Einträge *Administrationskonsole* und *Konfigurationsdateiassistent.*

30.3.3 SafeGuard Easy Clients installieren

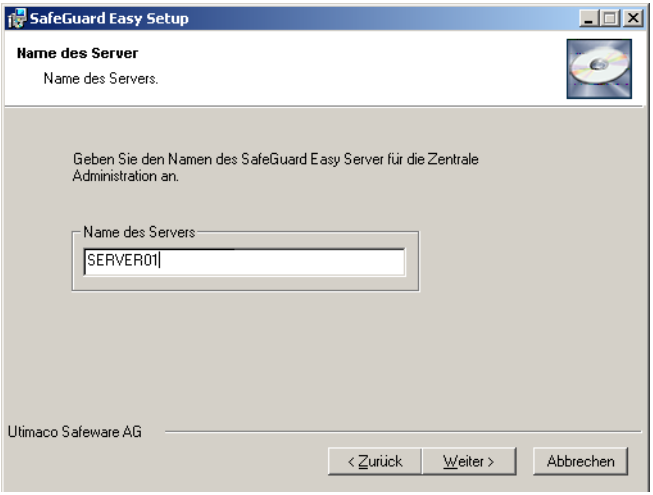
Die Installationsprozedur funktioniert wie gewohnt (siehe lokale oder zentrale Installation). Zur Kommunikation mit dem Server muss den Clients jedoch der UNC NETBIOS Name des SafeGuard Easy Servers und der sog. „Netzwerkagent“ (Server Anbindung) mitgegeben werden, der die Kommunikation mit dem Server ermöglicht.

Der Netzwerkagent kann nach der Installation von SafeGuard Easy nicht mehr mitgegeben werden! Soll ein Client zentral administriert werden, muss SafeGuard Easy neu mit aktivierter Server-Anbindung installiert werden.

Starten Sie die Installation durch Aufrufen von `Sgeasy.msi` aus dem CD-Verzeichnis \CLIENT (interaktive Installation). Wählen Sie im Rahmen einer „Angepassten“ Installation neben den bereits selektierten Komponenten die Option „Server Anbindung“ aus.



Im weiteren Verlauf der Installation tragen Sie im Dialog Server den UNC NETBIOS Name des SafeGuard Easy Servers ein (z.B. „Server01“).



Setzen Sie die Installation wie unter „Lokale Installation“ beschrieben fort. Sobald Sie fertig sind, müssen Sie ihr System neu starten.

ACHTUNG:
Wird der Name des SafeGuard Easy Clients nach der SafeGuard Easy Installation geändert, erkennt der Server den Client nicht mehr. Als Folge muss der „alte“ SafeGuard Easy Client Eintrag aus der SafeGuard Easy Datenbank gelöscht werden und der Client neu registriert werden.

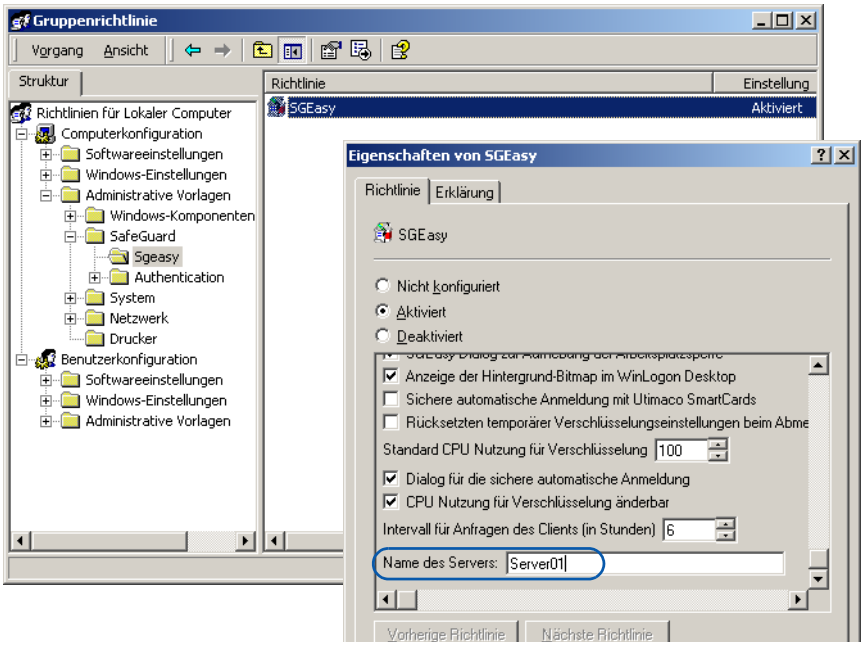
Servernamen nachträglich angeben

Wenn der Servername noch nicht bekannt ist, kann er nachträglich mit Standard-Windows-Mechanismen zentral am Client angepasst werden, denn es handelt sich um einen Eintrag in Utimacos administrative Vorlage.

Sie finden die Richtlinie unter

Computerkonfiguration
\Administrative Vorlagen
\SafeGuard
\SGEasy

Auf der Eigenschaftenseite von „SGEasy“ ist unter „Name des Servers“ der aktuelle SafeGuard Easy Server einzutragen.



30.3.4 Maximale Kapazität der SafeGuard Easy Datenbank

Die SafeGuard Easy Datenbank ist in der Grundeinstellung eine Microsoft Access Datenbank. Die Größe einer Microsoft Access Datenbank ist begrenzt auf 2 GB, kann aber erweitert werden durch Verweis auf andere Datenbanken.

Ein SafeGuard Easy Client beansprucht nach der Registrierung ungefähr 5 bis 7 KB des Speicherplatzes der Datenbank. Das bedeutet für 50.000 Clients ca. 340 bis 350 MB.

Wir empfehlen jedoch nicht, eine so große Anzahl an Arbeitsstationen mit einer einzigen (Server) Datenbank zu administrieren, sondern eine passende Organisations- und Administrationstruktur einzuführen, bei der die Arbeitsstationen über mehrere Server verwaltet werden.

30.3.5 SafeGuard Easy Server/Datenbank wiederherstellen

Für die erfolgreiche Wiederherstellung des SafeGuard Easy-Servers ist folgendes zu beachten:

- Folgende Dateien sichern, die sich standardmäßig im Produktverzeichnis befinden (C:\Programme\Utimaco\SafeGuard Easy):
  - Sgeasy.mdb
  - WksInfo.stg
  - Pubkey.sto
- NetBIOS Name und die IP-Adresse des (alten) SafeGuard Easy-Servers für Wiederherstellungszwecke notieren.

Mit Hilfe der gesicherten Dateien, NetBIOS und IP-Adresse können Sie beim erneuten Aufsetzen eines SafeGuard Easy-Servers den Stand der letzten Sicherung der Dateien wiederherstellen.

Dabei sind folgende Punkte zu beachten:

1. Dem neuen PC (Server) die gleiche IP-Adresse und den gleichen NetBIOS Namen zuweisen.
2. Anschließend den SafeGuard Easy-Server (Server.msi) neu installieren.
3. Nach abgeschlossener Installation den PC **nicht sofort neu starten**.
4. Die drei gesicherten Dateien in das Produktverzeichnis von SafeGuard Easy einspielen.
5. PC neu starten.
6. Nach dem Neustart die Administrationskonsole von SafeGuard Easy öffnen. Die Einträge der SafeGuard Easy Clients sind wieder vorhanden.

30.4 Microsoft SQL Server-Unterstützung

Als Standard-Datenbanktyp für das Speichern von Informationen über SafeGuard Easy Clients verwendet SafeGuard Easy eine Microsoft Access Datenbank. Mancher Anwender möchte vielleicht statt der Standardeinstellung einen anderen Datenbanktyp nutzen. SafeGuard Easy erfüllt diesen Kundenwunsch und erweitert das Spektrum der unterstützten Datenbanken um den Microsoft SQL Server.

Es gibt zwei Phasen für die Einrichtung der Microsoft SQL Server Unterstützung:

- Zuerst muss eine leere SafeGuard Easy-Datenbank auf dem SQL Server erzeugt werden.
- Anschließend muss diese leere Datenbank auf dem SafeGuard Easy Server registriert werden.

30.4.1 Wichtige Hinweise

- Der Microsoft SQL Server wird erst ab SafeGuard Easy 4.11 unterstützt.
- Der Microsoft SQL Server kann, muss aber nicht auf der Maschine installiert sein, auf der der SafeGuard Easy Server später installiert wird.
- Wenn geplant ist, eine SQL-Datenbank zu verwenden, dürfen solange keine SafeGuard Easy Clients installiert oder registriert werden bis als Standard-Datenbank der Microsoft SQL Server definiert wurde.
- Entwickelt und getestet wurde die Unterstützung für SQL Server mit folgenden Versionen:
  - SQL Server 2005
  - SQL Server Enterprise Edition 8.00.760 (Service Pack 3)

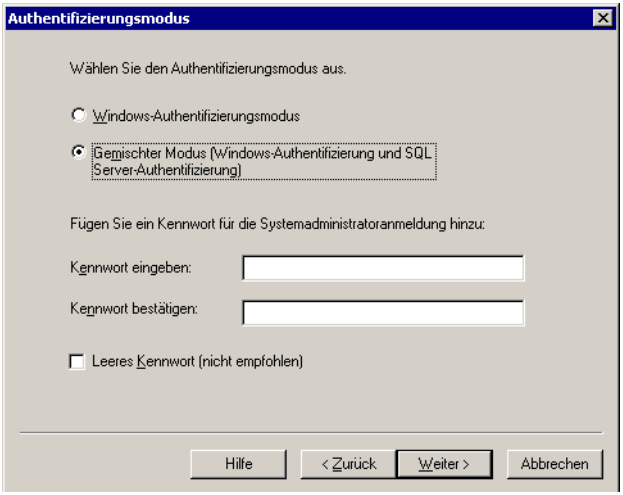
– SQL Server Developer Edition8.00.194 (RTM)

30.4.2 Leere SafeGuard Easy-Datenbank auf dem SQL-Server erzeugen

HINWEIS:
Unbedingt VOR der SafeGuard Easy Server Installation durchführen!

1. SQL Server installieren (wenn nicht schon vorhanden).

   Bei der Installation folgendes beachten:
   Als „Authentifizierungsmodus“ die Option „Gemischter Modus“ wählen.

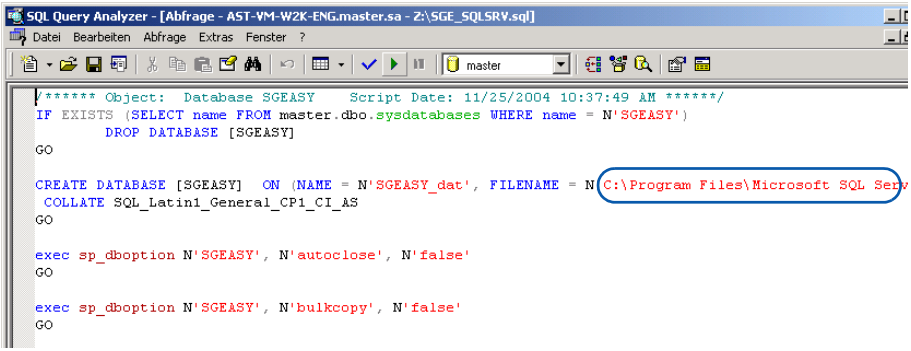


   Der Authentifizierungsmodus kann auch nach der SQL Server Installation umgestellt werden.

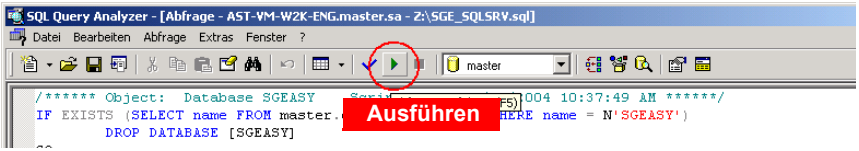
2. SQL Query Analyzer über **Programme / Microsoft SQL Server / Query Analyzer** aufrufen.

3. Die Datei `SGE_SQLSRV.sql` im Query Analyzer öffnen.
   `SGE_SQLSRV.sql` befindet sich in der Datei `SQL-info.zip` im Verzeichnis \TOOLS.
   `SGE_SQLSRV.sql` enthält das Skript, das benötigt wird, um eine leere SafeGuard Easy Datenbank auf dem SafeGuard Easy Server zu erzeugen. Diese Datenbank wird später als SafeGuard Easy Datenbank vom SafeGuard Easy Server genutzt.

   Die Einträge „C:\Program Files\Microsoft SQL Server“ mit dem Installationsverzeichnis des SQL Servers auf Ihrem PC überschreiben (z.B. „D:\Microsoft SQL Server“).

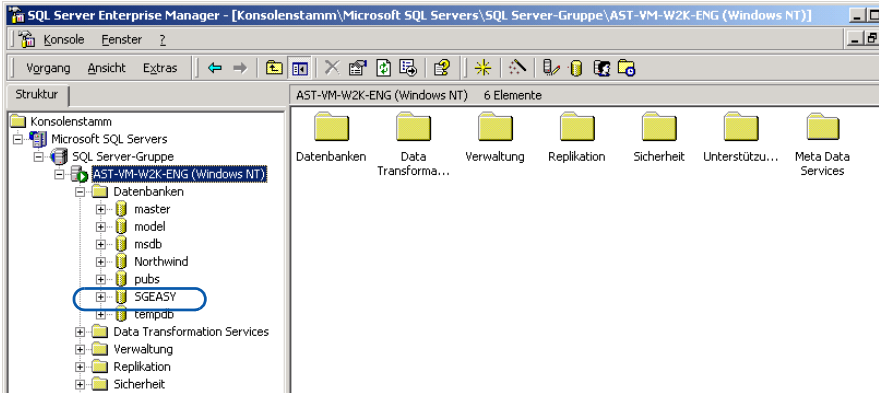

SQL Query Analyzer - [Abfrage - AST-VM-W2K-ENG.master.sa - Z:\SGE_SQLSRV.sql]
Datei Bearbeiten Abfrage Extras Fenster ?
master
/****** Object: Database SGEASY Script Date: 11/25/2004 10:37:49 AM ******/
IF EXISTS (SELECT name FROM master.dbo.sysdatabases WHERE name = N'SGEASY')
DROP DATABASE [SGEASY]
GO
CREATE DATABASE [SGEASY] ON (NAME = N'SGEASY_dat', FILENAME = N'C:\Program Files\Microsoft SQL Serv
COLLATE SQL_Latin1_General_CP1_CI_AS
GO
exec sp_dboption N'SGEASY', N'autoclose', N'false'
GO
exec sp_dboption N'SGEASY', N'bulkcopy', N'false'
GO

4. Das Skript ausführen.

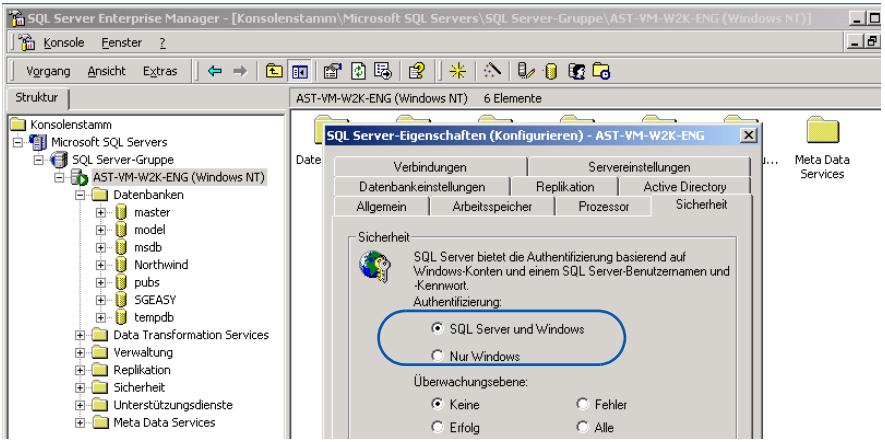

SQL Query Analyzer - [Abfrage - AST-VM-W2K-ENG.master.sa - Z:\SGE_SQLSRV.sql]
Datei Bearbeiten Abfrage Extras Fenster ?
master
Ausführen
/****** Object: Database SGEASY
IF EXISTS (SELECT name FROM master.
DROP DATABASE [SGEASY]

5. Nach Ausführen des Skripts den SQL Enterprise Manager aufrufen über **Programme / Microsoft SQL Server / Enterprise Manager**.

6. In Ihrem SQL Server wurde eine leere SafeGuard Easy-Datenbank mit Namen „SGEASY“ erzeugt.



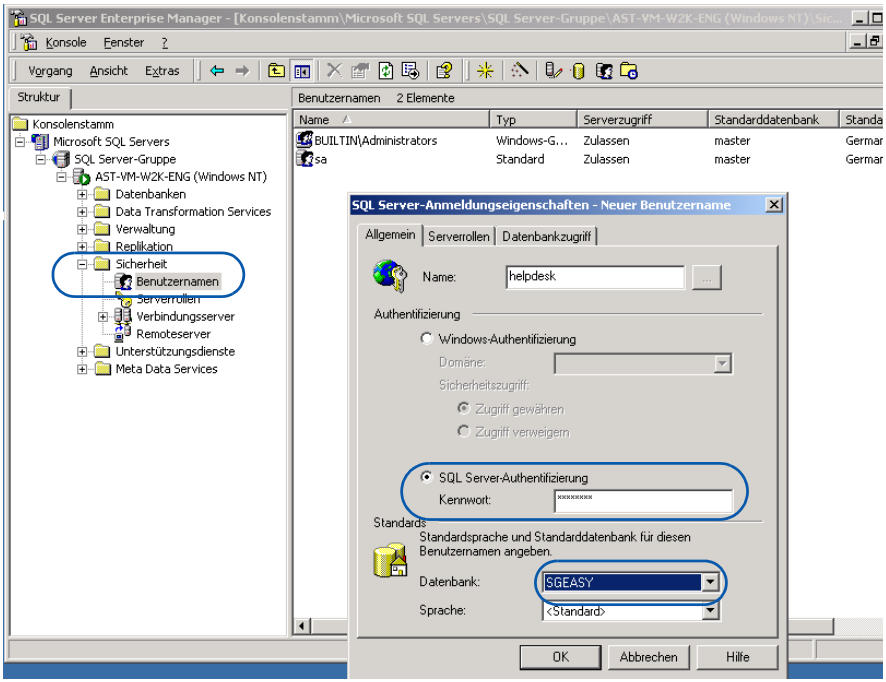
7. Wenn nicht bereits während der SQL Server Installation geschehen: In der Baumstruktur den eigenen SQL-Server wählen (im Beispiel „AST-VM-W2K-ENG (Windows NT)“ und über das Kontextmenü die Eigenschaften-Seite anzeigen lassen.



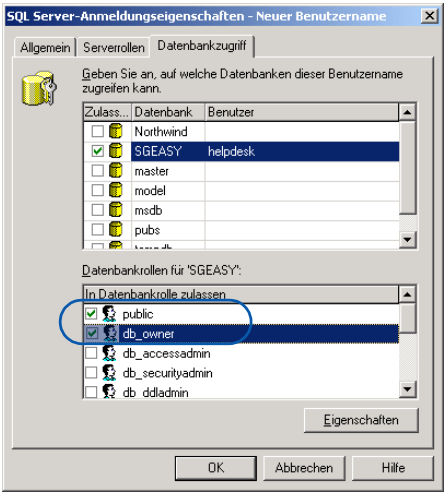
In der Registerkarte „Sicherheit“ die Authentifizierung auf „SQL Server und Windows“ setzen.

8. Optional: Ein anderes als das Standard-Systemkonto (Standard ist Benutzer „sa“) für die SGEASY-Datenbank wird erzeugt über Sicherheit > Benutzernamen > Kontextmenüeintrag „Neuer Benutzer“.

   In der Registerkarte „Allgemein“ unter „Authentifizierung“ die Option „SQL Server Authentifizierung“ wählen und das Kennwort eingeben. Als „Datenbank“ SGEASY einstellen.



In der Registerkarte „Datenbankzugriff“ als zugelassene Rollen „public“ und „owner“ markieren.



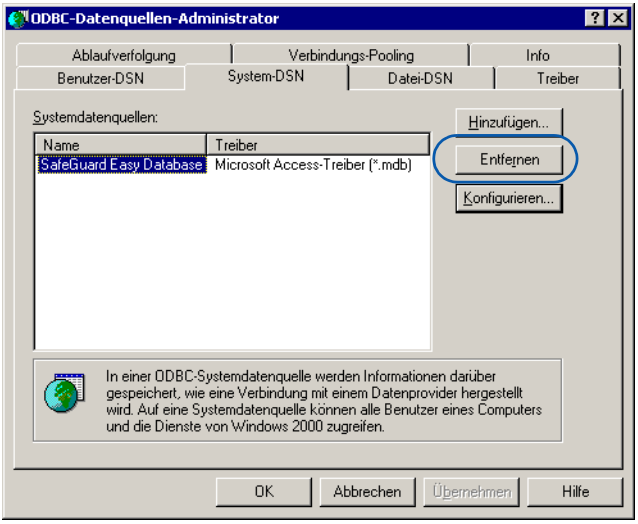
30.4.3 Neue (leere) SafeGuard Easy-Datenbank auf dem SafeGuard Easy Server registrieren

1. SafeGuard Easy Server installieren durch Aufrufen der Datei `Server.msi` aus dem \SERVER Verzeichnis der Produkt-CD. Optional kann zusätzlich zum Server die Administrationskonsole installiert werden.

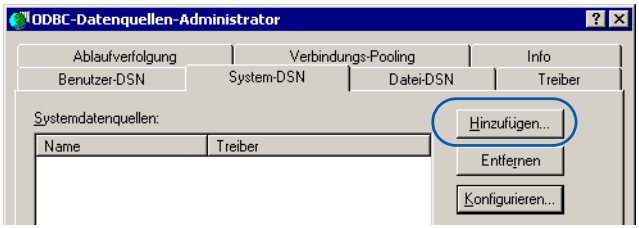
> ***WICHTIG:***
> Den PC nach der SafeGuard Easy Server-Installation NICHT neu starten!

2. Nacheinander **Einstellungen / Systemsteuerung / Verwaltung / Datenquellen (ODBC)** aufrufen.

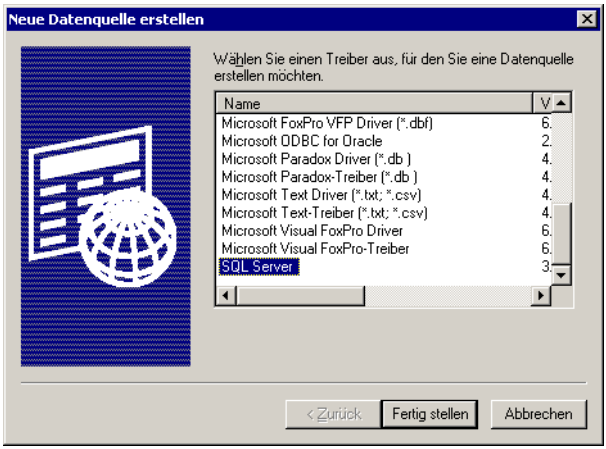
3. Die Registerkarte „System-DSN“ öffnen und die Standard „SafeGuard Easy Database“ mit dem Microsoft Access Treiber aus der Liste entfernen.



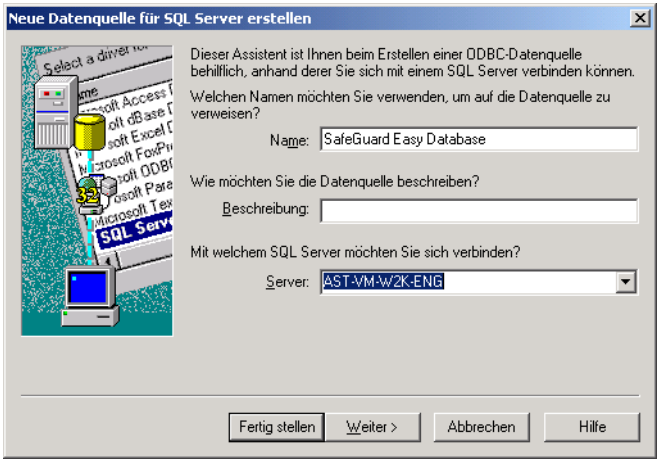
4. Eine neue Datenquelle erstellen über [Hinzufügen] in der Registerkarte System-DSN.



5. Als Treiber „SQL Server“ wählen. Alle Dialoge mit [Weiter] bestätigen.

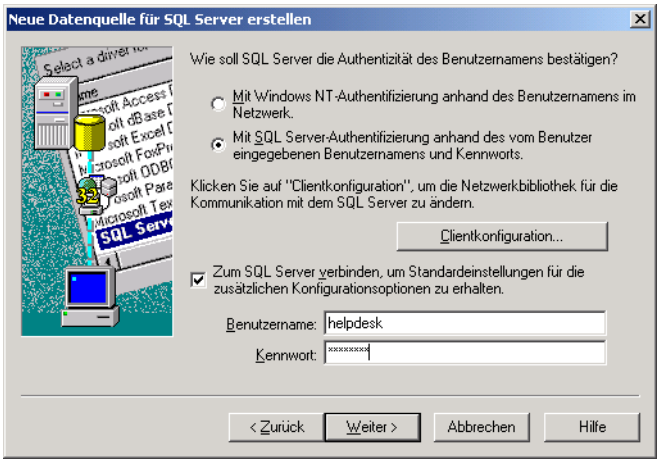


6. Verbindung mit SQL Server erstellen.

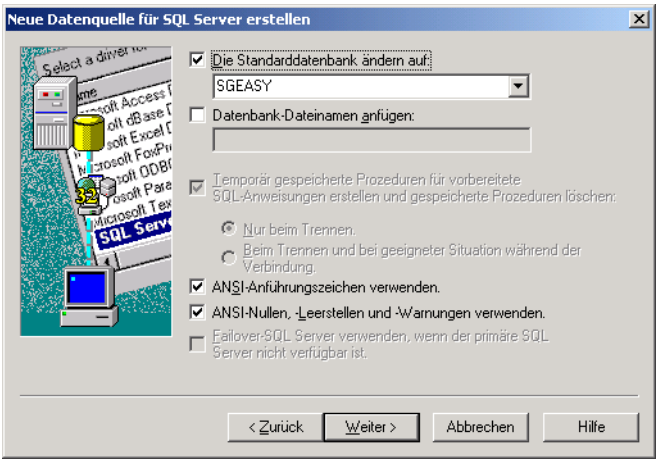

Neue Datenquelle für SQL Server erstellen
Dieser Assistent ist Ihnen beim Erstellen einer ODBC-Datenquelle behilflich, anhand derer Sie sich mit einem SQL Server verbinden können.
Welchen Namen möchten Sie verwenden, um auf die Datenquelle zu verweisen?
Name: SafeGuard Easy Database
Wie möchten Sie die Datenquelle beschreiben?
Beschreibung:
Mit welchem SQL Server möchten Sie sich verbinden?
Server: AST-VM-W2K-ENG
Fertig stellen
Weiter >
Abbrechen
Hilfe

HINWEIS:
Der Name der Datenbank muss zwingend "SafeGuard Easy Database" sein.

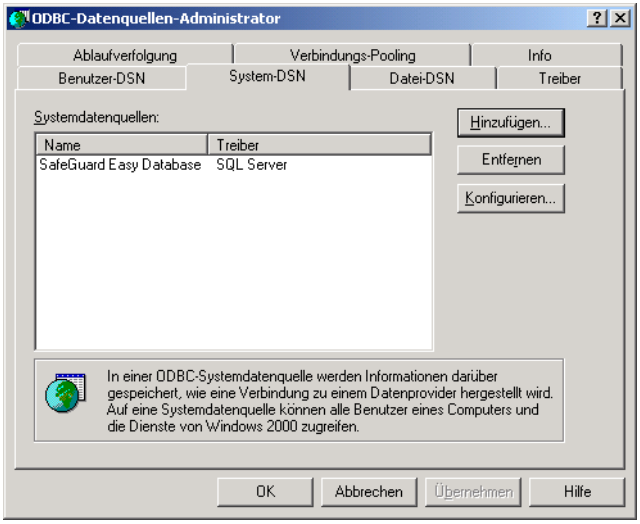
7. Die Option „Mit SQL Server-Authentifizierung...“ wählen und Standardbenutzer für die SQL-Datenbank wählen (i.d.R. Benutzer „sa“ oder im Beispiel Benutzer „helpdesk“).


Neue Datenquelle für SQL Server erstellen
Wie soll SQL Server die Authentizität des Benutzernamens bestätigen?
Mit Windows NT-Authentifizierung anhand des Benutzernamens im Netzwerk.
Mit SQL Server-Authentifizierung anhand des vom Benutzer eingegebenen Benutzernamens und Kennworts.
Klicken Sie auf "Clientkonfiguration", um die Netzwerkbibliothek für die Kommunikation mit dem SQL Server zu ändern.
Clientkonfiguration...
Zum SQL Server verbinden, um Standardeinstellungen für die zusätzlichen Konfigurationsoptionen zu erhalten.
Benutzername: helpdesk
Kennwort: ********
< Zurück
Weiter >
Abbrechen
Hilfe

8. Als Standarddatenbank „SGEASY“ auswählen und die anderen Standardeinstellungen behalten.


Neue Datenquelle für SQL Server erstellen
Die Standarddatenbank ändern auf:
SGEASY
Datenbank-Dateinamen anfügen:
Temporär gespeicherte Prozeduren für vorbereitete SQL-Anweisungen erstellen und gespeicherte Prozeduren löschen:
Nur beim Trennen.
Beim Trennen und bei geeigneter Situation während der Verbindung.
ANSI-Anführungszeichen verwenden.
ANSI-Nullen, -Leerstellen und -Warnungen verwenden.
Failover-SQL Server verwenden, wenn der primäre SQL Server nicht verfügbar ist.
< Zurück
Weiter >
Abbrechen
Hilfe

9. Als „neuer“ SafeGuard Easy Datenbanktyp ist nun die SQL-Datenbank eingetragen.

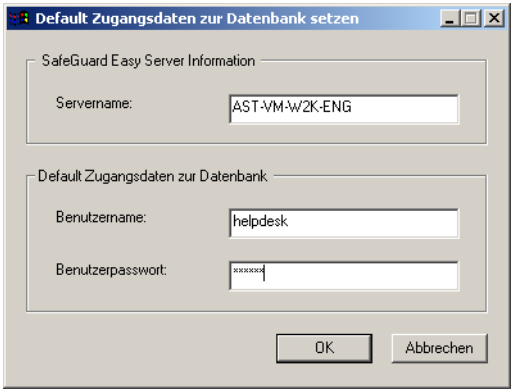


10. Das System neu starten und die SGEasy Services `SgeSrv.exe` und `CfgDBSrv.exe` stoppen (SgeSrv.exe=SafeGuard Easy Server und CfgDBSrv.exe=SafeGuard Easy Database Server).

11. Die Zugangsdaten des Standardbenutzers zur SafeGuard Easy Datenbank werden nicht im Klartext übermittelt. Das Tool `SetDBPwd.exe` aktualisiert den Standardbenutzer und speichert das Passwort in die verschlüsselte Datei `DBPwd.stg`, damit es vom SafeGuard Easy Server genutzt werden kann.

ACHTUNG:
Wenn der Standard-Datenbankbenutzer sich OHNE Passwort anmeldet, sind die Schritte 10 und 11 nicht notwendig!

Nach dem Start von `SetDBPwd.exe` aus dem SafeGuard Easy Server Installationsverzeichnis erscheint ein Dialog zur Dateneingabe.



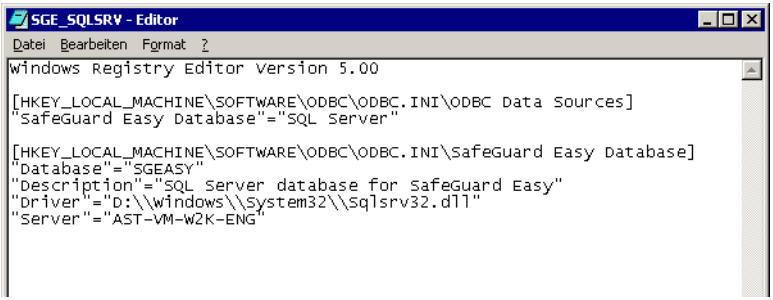
HINWEISE:

- Im Feld „Servername“ muss der Name (oder die IP-Adresse) des PCs stehen, auf dem der SafeGuard Easy Server installiert ist (im Beispiel sind SafeGuard Easy Server und SQL Server auf derselben Maschine installiert).
- Unter „Default Zugangsdaten zur Datenbank“ müssen die Benutzerdaten für die SGEASY-Datenbank am SQL Server eingetragen werden!
  Wenn statt des Standardbenutzers (in unserem Beispiel „helpdesk“) ein anderes Benutzerkonto anmelden will, muss dieses für die SGEASY-Datenbank vorhanden sein und über entsprechende Rechte verfügen.

12. PC neu starten.

Die Schritte 4 bis 7 können auch folgendermaßen durchgeführt werden:

1. Registrierungsdatei `SGE_SQLSRV.reg` öffnen (zu finden in der Datei `SQL-info.zip` im Verzeichnis \TOOLS).



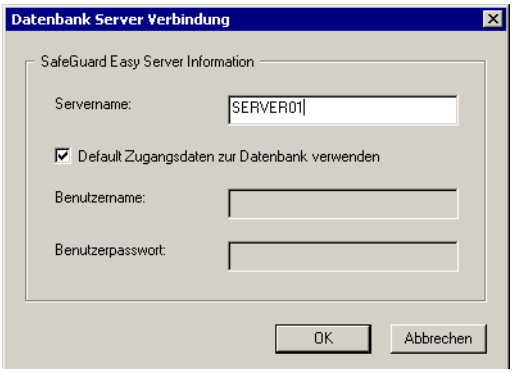
2. Die folgenden Schlüssel ändern:
   - „Driver“
     Korrekten Pfad für die Datei `SQLSRV32.dll` auf Ihrem SafeGuard Easy Server eingeben (z.B. „D:\\Windows\\System32\\SQLSRV32.dll“)
   - „Server“
     Namen des SQL Servers angeben
     (z.B. „AST-VM-W2K-ENG).
3. `SGE_SQLSRV.reg` ausführen.

31 Administrationskonsole

Bevor mit der Datenbank gearbeitet werden kann, muss über die Administrationskonsole eine Verbindung zum SafeGuard Easy Server hergestellt werden.

31.1 Anmelden an die SafeGuard Easy Datenbank

Nach Aufrufen der Administrationskonsole über **Start / Programme / Utimaco / SafeGuard Easy / Administrationskonsole** erscheint eine Anmeldemaske.



Folgende Informationen müssen dort eingetragen werden:

Servername
Name des SafeGuard Easy Servers, auf dem die SafeGuard Easy Datenbank liegt. Der Servername kann auch als IP-Adresse eingegeben werden.

Standard-Zugangsdaten zur Datenbank
Verwendet die aktuellen Standard-Anmeldedaten für die SafeGuard Easy Datenbank.
In der Grundeinstellung gelten diese Standardzugangsdaten:
Benutzername: Admin, Passwort:*Kein Passwort*

Andere Zugangsdaten sind nach dem Deaktivieren des Auswahlkästchens eingebbar.

Nach einer erfolgreichen Verbindung werden der Servername und der Benutzername (aber nicht die Datenbank oder das Passwort) in der Registry gespeichert und bei der nächsten Anmeldung automatisch wiederverwendet. Die Administrationskonsole verbindet sich aber nur automatisch mit dem SafeGuard Easy Server, wenn die letzte Anmeldung mit den „Standard-Zugangsdaten“ durchgeführt wurde.

Meistens befinden sich SafeGuard Easy Server und Administrationskonsole auf ein und derselben Maschine (ist aber nicht vorgeschrieben!). Wenn sie sich auf verschiedenen Maschinen befinden (SafeGuard Easy Server und Administrator-PC), erfolgt der Verbindungsaufbau über die Authentisierung mit Windows-Benutzerdaten, d.h. der gegenwärtig am Administrator-PC angemeldete Benutzer muss auch am SafeGuard Easy Server über ein entsprechendes Benutzerkonto verfügen.

31.1.1 Verbindung trennen und wiederaufnehmen

Ohne Standard-Benutzerdaten melden Sie sich an, wenn Sie über das **Menü Datei** in der Administrationskonsole die Verbindung zuerst **trennen** und dann **wiederaufnehmen**.

31.1.2 Standardzugangsdaten zur SafeGuard Easy Datenbank ändern

Weitere Informationen zu diesem Thema finden Sie in der Utimaco-Wissensdatenbank http://www.utimaco.de/myutimaco.

Nutzen Sie bitte die Suchfunktion der Wissensdatenbank, um nach Stichworten wie „Zugangsdaten & Datenbank“ zu suchen.

Die mit SafeGuard Easy gelieferte Datenbank ist eine Microsoft Access Datenbank. Sie wird während der Installation vom SafeGuard Easy Server registriert als eine ODBC Datenquelle mit dem Datenquellen-Namen (DSN) „SafeGuard Easy Database“. Die SafeGuard Easy Datenbank nutzt den Standard ODBC Treiber für Microsoft Access, der in Ihre Windows-Version integriert ist. Da der ODBC-Treiber für Microsoft Access bereits in der Grundeinstellung für Windows 2000 und Windows XP installiert ist, ist es nicht nötig, MS Access zu installieren, um Zugriff auf die SafeGuard Easy Datenbank zu erhalten. Wenn Sie jedoch aus bestimmten Gründen die Standard-Anmeldedaten für Ihre Datenbank ändern wollen, muss Microsoft Access installiert sein, um eine Benutzerdaten-Datei zu erstellen.

Eine Microsoft Access Benutzerdaten-Datei enthält Informationen über Benutzer, Passwörter und Gruppenzugehörigkeit. Eine Benutzerdaten-Datei hat in der Grundeinstellung die Dateierweiterung .MDW und wird von Microsoft auch als „Workgroup Information File“ bezeichnet. Eine Microsoft Access Installation erzeugt das Standard Workgroup Information File `System.mdw` und legt es ab unter

- MS Access 97 \WinNT\System32
- MS Access 2000 \Programme\Gemeinsame Dateien\System

Das MS Access-Tool `Wrkgadm.exe` kann eine neue MDW-Datei erzeugen, und diese wird dann als SafeGuard Easy-Benutzerdatei verwendet. Sie können aber auch die Standard-MDW-Datei verwenden.

`Wrkgadm.exe` ist zu finden unter

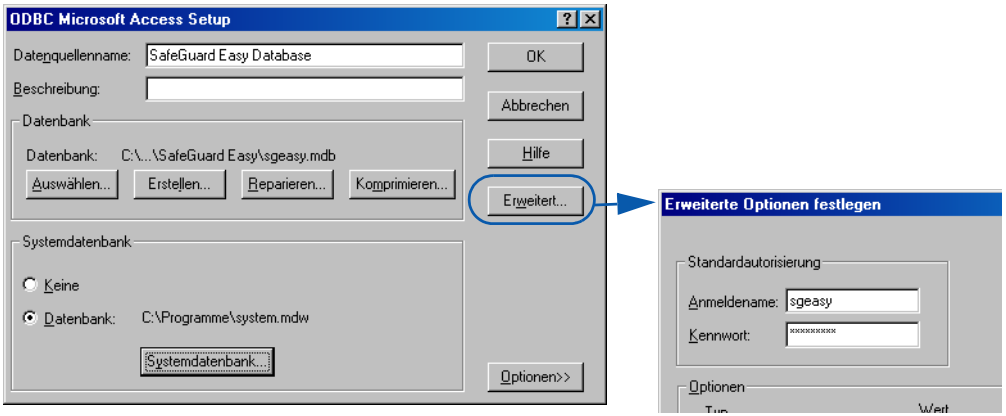
- MS Access 97 \WinNT\System32\
- MS Access 2000 \Progamme\Microsoft Office\Office\1033\

Wenn Sie die Standard-MDW-Datei benutzen, öffnen Sie MS Access. Unter Werkzeuge / Sicherheit wählen Sie die Option „Benutzer- und Gruppenkonten“. Hier können Sie Benutzer, Passwörter und die Gruppenzugehörigkeit bestimmen.
Danach öffnen Sie die SafeGuard Easy Datenbank `Sgeasy.mdb` mit Microsoft Access. Im Menü Werkzeuge / Sicherheit wählen Sie „Benutzer- und Gruppenberechtigungen“. Hier können Sie dann den definierten Benutzern Zugriffsrechte zuweisen.

In der Grundeinstellung verbindet SafeGuard Easy die SafeGuard Easy Datenbank nicht mit einer MDW-Datei. In diesem Fall werden als Standard-Anmeldedaten der Benutzername „Admin“ ohne Passwort verwendet.

Um andere Anmeldedaten zuzulassen, rufen Sie **Programme/Systemsteuerung/Verwaltung/Datenquellen (ODBC)/System-DSN/Konfigurieren** auf. Tragen Sie unter System-Datenbank die Standard-MDW-Datei `System.mdw` ein. Über die Schaltfläche „Erweitert...“ können auch geänderte Standardanmeldedaten eingetragen werden.

Beachten Sie bitte, dass das als Standard eingetragene Benutzerprofil auch als berechtigter Benutzer der Datenbank existiert.



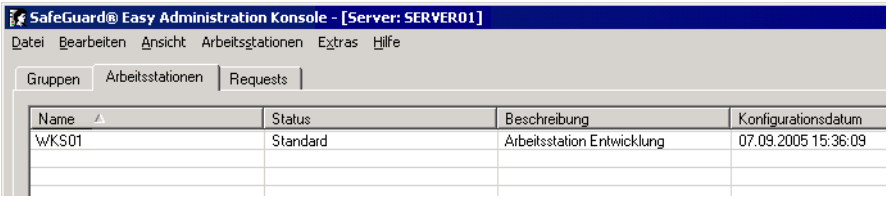
31.2 Benutzeroberfläche

Nach erfolgreicher Anmeldung an die SafeGuard Easy Datenbank erscheint das Administrationsfenster der Administrationskonsole mit den Registerkarten Arbeitsstationen, Gruppen und Requests. Ein Wechsel zwischen den einzelnen Registerkarten ist über einen einfachen Klick auf die entsprechende Registerkarte oder das **Menü Ansicht** möglich.

Arbeitsstationen

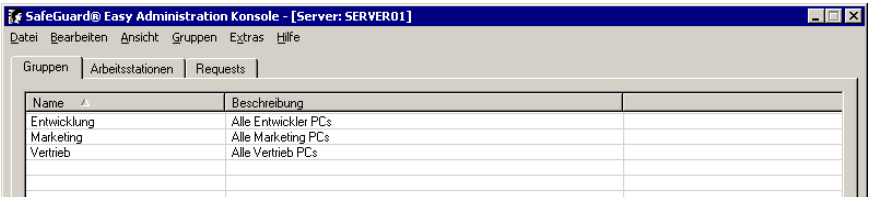
Zeigt eine Liste aller SafeGuard Easy Clients, die sich am Server authentisiert haben.

- **Name:** UNC Netbios Name der registrierten Arbeitsstation.
- **Beschreibung:** Detaillierte Angaben zur registrierten Arbeitsstation
- **Status:** Arbeitsstation ist online (Standard) oder offline
- **Konfigurationsdatum:** Zeigt an, wann (Datum, Uhrzeit) ein SafeGuard Easy Client zuletzt seine aktuellen Konfigurationsdaten an den SafeGuard Easy Server gesendet hat.



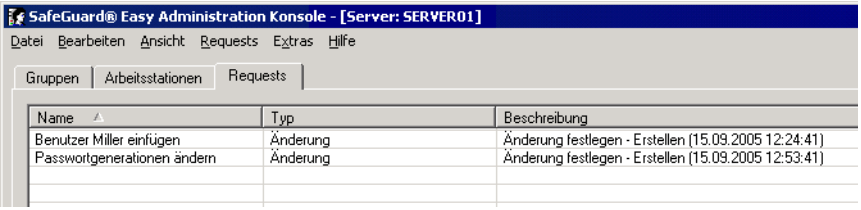
Gruppen

Zeigt alle angelegten SafeGuard Easy Gruppen, in denen einzelne SafeGuard Easy Clients zusammengefasst sind.

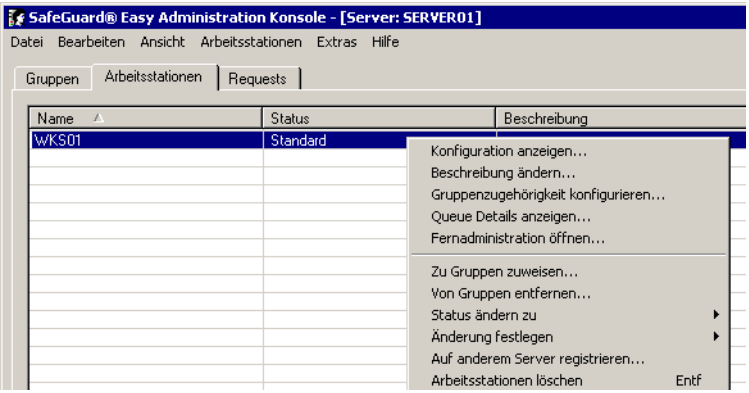


Requests

Zeigt eine Liste aller erstellten Konfigurationsänderungen, die auf SafeGuard Easy Clients ausgeführt wurden/werden.


SafeGuard® Easy Administration Konsole - [Server: SERVER01]
Datei Bearbeiten Ansicht Requests Extras Hilfe
Gruppen Arbeitsstationen Requests
Name Typ Beschreibung
Benutzer Miller einfügen Änderung Änderung festlegen - Erstellen (15.09.2005 12:24:41)
Passwortgenerationen ändern Änderung Änderung festlegen - Erstellen (15.09.2005 12:53:41)

Die wichtigsten Kommandos für eine Arbeitsstation, Gruppe oder einen Request sind in deren Kontextmenü verfügbar. All diese Kommandos sind auch über die verschiedenen Menüs (Arbeitsstation, Gruppen, Requests) aufrufbar. Die Menüs werden entsprechend der Wahl der Registerkarte angezeigt (Aktive Registerkarte Arbeitsstation zeigt Menü Arbeitsstation an etc.).

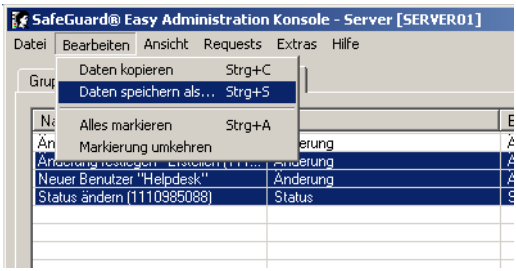


Sobald mehrere Arbeitsstationen, Gruppen, Requests vorhanden sind, ist eine Mehrfachselektion über bekannte Windows-Mechanismen (STRG-/Umschalt-Taste oder über das **Menü Bearbeiten** möglich.

Aus der Administrationskonsole kann auch die **Remote Administration** aufgerufen werden (**Menü Arbeitsstation / Fernadministration öffnen**). Details zur Remote Administration lesen Sie bitte im Kapitel 'Remote Administration'.

31.2.1 Inhalt der Registerkarten als Textdatei speichern

Die Administrationskonsole stellt eine Funktionalität bereit, die es erlaubt den Inhalt der momentan aktiven Registerkarte (Gruppen, Arbeitsstationen oder Requests) in einer Text-Datei abzuspeichern oder in der Zwischenablage zu „kopieren“. Text-Datei und Inhalt der Zwischenablage können in ein beliebiges Programm importiert und aufbereitet werden. Die Funktionalität ist aktiv, sobald eine Gruppe, Arbeitsstation oder ein Request selektiert ist. Das Speichern des Registerkarteninhalts eignet sich vor allem für Archivierungs-/Auswertungszwecke.



Aufgerufen wird die Kopier- und Speicherfunktion über das **Menü Bearbeiten** in der Administrationskonsole.

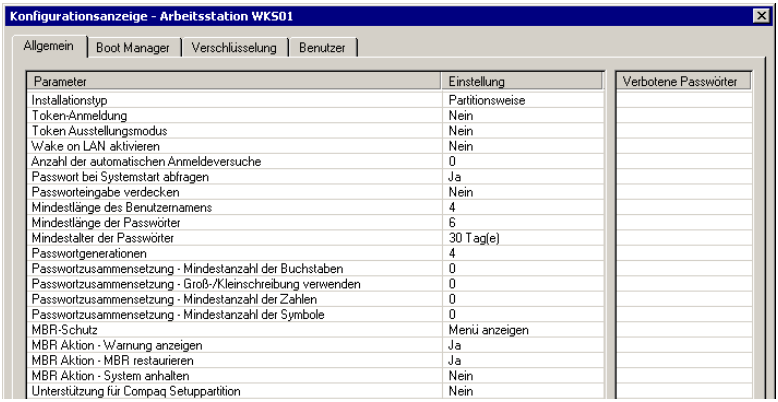
- Der Unterpunkt **Daten speichern als** erstellt eine ASCII-Datei, die mit beliebigem Namen in einem Verzeichnis abgelegt werden kann. Diese Datei enthält die Spaltenüberschriften plus markierter Registerkarteneinträge.
- Der Unterpunkt **Daten kopieren** „parkt“ die markierten Registerkarteneinträge (ohne Spaltenüberschriften) in der Zwischenablage. Die Zwischenablage kann in jedes beliebige Programm eingefügt werden.

31.3 Aktuelle Konfiguration eines registrierten SafeGuard Easy Clients anzeigen

Sobald sich SafeGuard Easy Client und SafeGuard Easy Server erfolgreich authentisiert haben, darf der an der Administrationskonsole angemeldete Benutzer die SafeGuard Easy Einstellungen des Clients einsehen.

Zum Überprüfen aktueller Einstellungen oder zur Vorbereitung von Änderungen ist es immer ratsam, sich zunächst einen Überblick über aktuelle Konfigurationen zu verschaffen. Desweiteren lässt sich auch über diese Funktion leicht kontrollieren, ob Requests tatsächlich erfolgreich auf Clients ausgeführt wurden oder nicht.

1. Wechseln Sie in die Registerkarte **Arbeitsstation** und wählen einen SafeGuard Easy Client aus.
2. Das **Menü Arbeitsstation/Konfiguration anzeigen** wählen.
3. Es erscheint ein Fenster mit vier Registerkarten, die identisch sind mit den Bezeichnungen in der SafeGuard Easy Administration, nämlich: Allgemein, Verschlüsselung, Bootmanager und Benutzer. Jede Registerkarte zeigt die SafeGuard Easy Konfiguration am ausgewählten Client.



31.3.1 Beschreibung des Client ändern

Um einer in der Registerkarte „Arbeitsstationen“ angezeigten Arbeitsstation eine neue Beschreibung zu geben, öffnen Sie im **Menü Arbeitsstationen** den Befehl **Beschreibung ändern**. Die geänderten Einträge werden sofort übernommen.

31.3.2 Client löschen

Zum Löschen eines Client klicken Sie im **Menü Arbeitsstationen** auf **Arbeitsstation löschen**. Der Client wird dann aus der Liste der registrierten Arbeitsstationen entfernt.

31.4 SafeGuard Easy Client neu registrieren

Der Modus für die Neuregistrierung eines SafeGuard Easy Clients wird dann benötigt, wenn ein SafeGuard Easy Client dem SafeGuard Easy Server nicht bekannt ist.

In der Praxis könnte die Funktion z.B. in diesem Fall angewandt werden: In einem Unternehmen wird die SafeGuard Easy Datenbank jeden Tag um 5:00 Uhr gesichert. Um 8:00 Uhr registriert sich ein neuer SafeGuard Easy Client erfolgreich am SafeGuard Easy Server und um 10:00 Uhr gibt es einen Servercrash. Der SafeGuard Easy Server wird wiederhergestellt - allerdings mit der „alten“ Datenbanksicherung, die um 5:00 Uhr durchgeführt wurde. Diese Sicherung enthält nicht den neuen SafeGuard Easy Client, der sich um 8:00 registriert hatte. Über die Neuregistrierung wird der SafeGuard Easy Client der SafeGuard Easy Datenbank wieder hinzugefügt.

Damit die Neuregistrierung erfolgreich ist, muss der Benutzer der Administrationskonsole gültige SafeGuard Easy-Benutzerdaten des neuen SafeGuard Easy Client kennen und sich mit diesen am Client authentisieren.

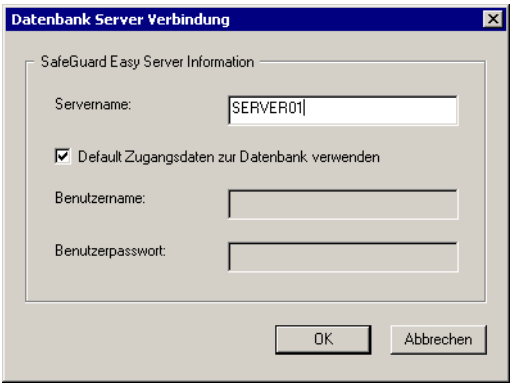
HINWEIS:
Es kann immer nur ein Client auf einmal neu registriert werden!

Voraussetzungen

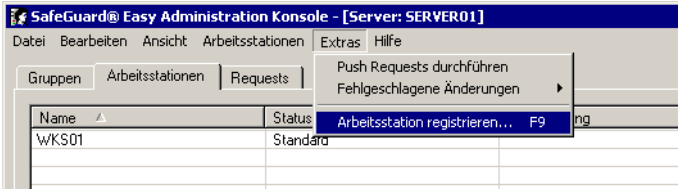
- Zwischen neuem SafeGuard Easy Client und SafeGuard Easy Server muss eine Netzwerkverbindung bestehen.
- SafeGuard Easy muss auf dem betreffenden SafeGuard Easy Client mit der Option „Server-Anbindung“ installiert sein.
- Der neue SafeGuard Easy Client darf nicht bereits auf dem Server registriert sein. Ist der neue SafeGuard Easy Client auf dem SafeGuard Easy Server bereits registriert und soll unbedingt nochmals registriert werden, muss der Client-Eintrag zuerst aus der Datenbank gelöscht und dann neu registriert werden. Gelöscht werden Clients aus der SafeGuard Easy Datenbank über das **Menü Arbeitsstationen / Arbeitsstationen löschen**.
- Der Benutzer der Administrationskonsole muss SafeGuard Easy-Zugangsdaten zum neuen SafeGuard Easy Client kennen.

Vorgehensweise

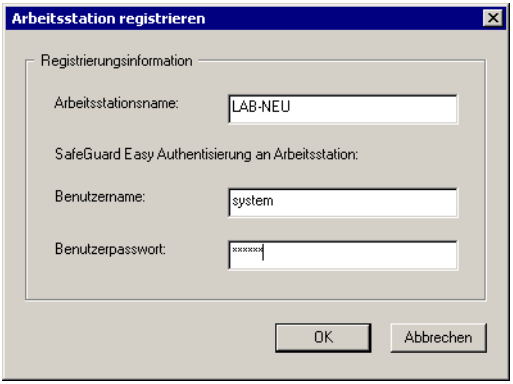
1. Netzwerkverbindung zwischen Client und Server sicherstellen.
2. Administrationskonsole starten und an Datenbank anmelden.



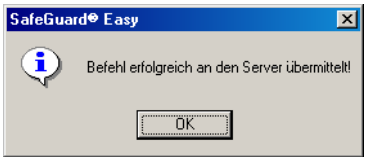
3. **Menü Extras / Arbeitsstation registrieren** aufrufen.



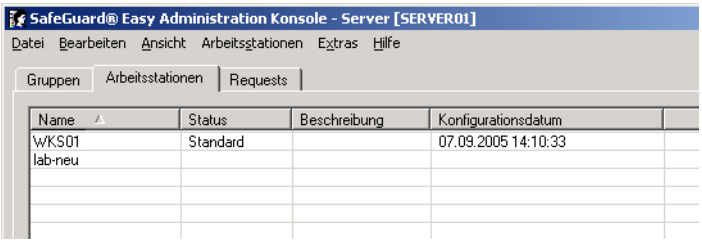
4. Ein Dialog erscheint, der den Namen des SafeGuard Easy Client und die Authentisierungsdaten zu diesem Client abfragt.
   Das Benutzerprofil des eingetragenen SafeGuard Easy-Benutzers muss am SafeGuard Easy Client existieren. Das Profil benötigt keine speziellen SafeGuard Easy-Rechte.



5. Angaben mit [OK] bestätigen. Erfolg/Misserfolg werden in einem Dialog angezeigt.



6. Der Client hinterlässt dann Informationen am SafeGuard Easy Server. Dies kann - je nach Netzwerkbelastung - einige Zeit in Anspruch nehmen. In der Administrationskonsole erscheint nach der Wartezeit der neue SafeGuard Easy Client (Die Anzeige in der Administrationskonsole kann auch über [F5] manuell aktualisiert werden).



31.4.1 Mehrere SafeGuard Easy Clients neu registrieren

Die Neuregistrierung funktioniert für alle SafeGuard Easy Clients ab der Version 4.11.

So registrieren Sie mehrere SafeGuard Easy Clients neu:

1. Erstellen Sie mit dem Konfigurationsdateiassistenten eine neue Konfigurationsdatei mit der Eigenschaft "Installieren".
2. Geben Sie in dieser Konfigurationsdatei das auf den SafeGuard Easy Clients eingestellte Passwort des Benutzers SYSTEM an.
3. Speichern Sie die Konfigurationsdatei unter "SGEREG.cfg" ab.
4. Kopieren Sie am SafeGuard Easy Client die Datei SGEREG.cfg in das Verzeichnis <Systemlaufwerk>/System 32.
5. Erstellen Sie am SafeGuard Easy Client unter

   HKEY_LOCAL_MACHINE
   SOFTWARE
   Utimaco
   Sgeasy

   zwei neue Registrierungseinträge [DWORD-Werte].

   NotRegistered=1
   RegReport=1
6. Starten Sie den SafeGuard Easy Client neu (oder den SafeGuard Easy Service).

31.5 SafeGuard Easy Clients auf einem anderen SafeGuard Easy Server registrieren

Wenn SafeGuard Easy Clients von einem anderen als dem bisherigen SafeGuard Easy Server administriert werden sollen, geschieht dies über die Funktion „Auf einem anderen Server registrieren“. Für die Umregistrierung wird ein sog. Registrierungsrequest erzeugt. Der Registrierungsrequest ist einem „regulären“ Request ähnlich, enthält aber statt Konfigurationsupdates den neuen SafeGuard Easy Servernamen und SafeGuard Easy-Zugangsdaten für die Authentisierung am SafeGuard Easy Client, der „verschoben“ werden soll.

Die Abarbeitung eines Registrierungsrequests entspricht prinzipiell dem eines „regulären“ Requests: Nach Fertigstellung reiht die Administrationskonsole den Registrierungsrequest in die Warteschleife ein. Sobald ein SafeGuard Easy Client am „alten“ SafeGuard Easy Server nachfragt, findet er dort den Registrierungsrequest, den er an den „neuen“ SafeGuard Easy Server schickt. Anschließend erhält der alte SafeGuard Easy Server vom SafeGuard Easy Client einen Bericht über die Neuregistrierung, woraufhin der SafeGuard Easy Client aus der „alten“ SafeGuard Easy Datenbank entfernt wird.

HINWEISE:

Der neue SafeGuard Easy Server darf nicht als SafeGuard Easy Client am alten SafeGuard Easy Server registriert sein.

Einzelne oder mehrere SafeGuard Easy Clients, aber auch Gruppen sind verschiebbar.

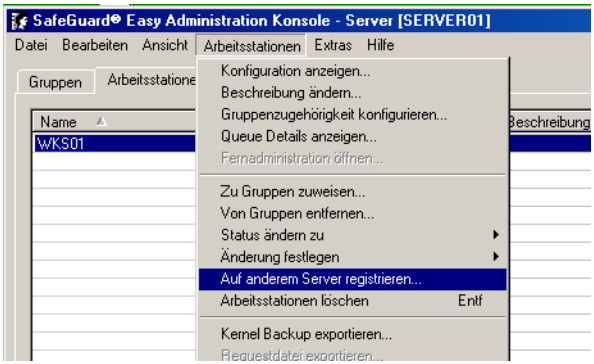
Nach erfolgreichem Verschieben des SafeGuard Easy Clients wird der Registrierungsrequest gelöscht, da der SafeGuard Easy Client dann dort nicht mehr existiert. Der Registrierungsrequest bleibt nur bis zu dem Zeitpunkt in der Warteschleife, solange der Registrierungsrequest auf „Wartend“, „Geplant“ oder „Fehlgeschlagen“ steht.

Voraussetzungen

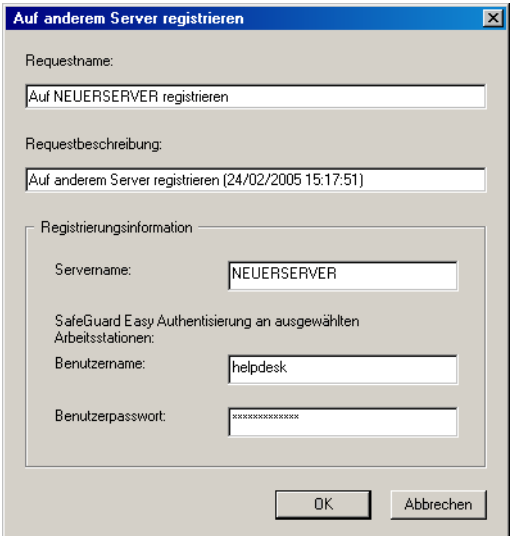
- Zwischen SafeGuard Easy Client und SafeGuard Easy Server muss eine Netzwerkverbindung bestehen.
- Der Benutzer der Administrationskonsole muss die SafeGuard Easy-Zugangsdaten zum SafeGuard Easy Client kennen.
- Der SafeGuard Easy Client muss bereits auf dem alten SafeGuard Easy Server registriert sein (= muss bereits in der SafeGuard Easy Datenbank vorhanden sein).

Vorgehensweise

1. Administrationskonsole starten und an Datenbank anmelden.
2. Ausgewählte Clients/Gruppen markieren.
3. Menü **Arbeitsstationen (Gruppen) / Auf anderem Server registrieren** aufrufen.

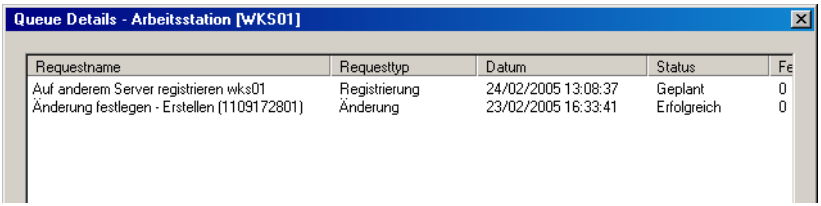


4. Ein Dialog erscheint, der den Namen des neuen SafeGuard Easy Servers und die Authentisierungsdaten zu dem Client abfragt. Requestname und -beschreibung sollten aussagekräftig sein. Das Benutzerprofil des eingetragenen SafeGuard Easy-Benutzers muss am SafeGuard Easy Client existieren, aber keine speziellen SafeGuard Easy-Rechte besitzen.

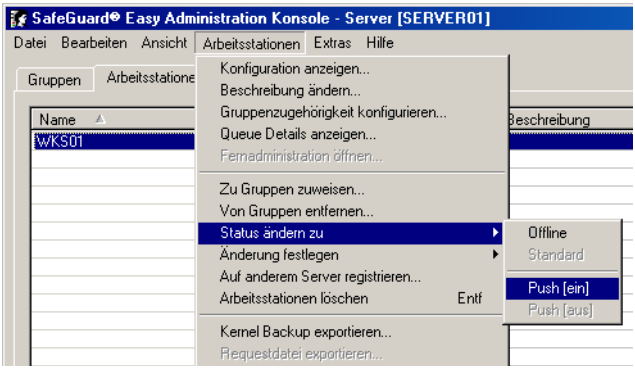


5. Angaben mit [OK] bestätigen.

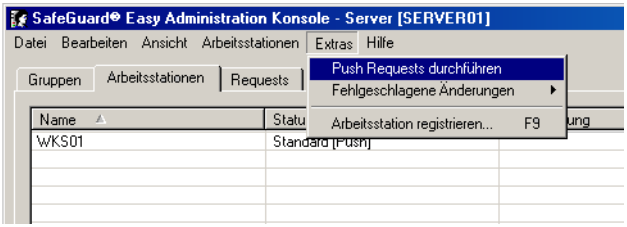
6. Der Registrierungsrequest erscheint in der Warteschleife.



7. Status des SafeGuard Easy Client auf „Push“ setzen über das **Menü Arbeitsstationen / Status ändern zu / Push [ein]**.

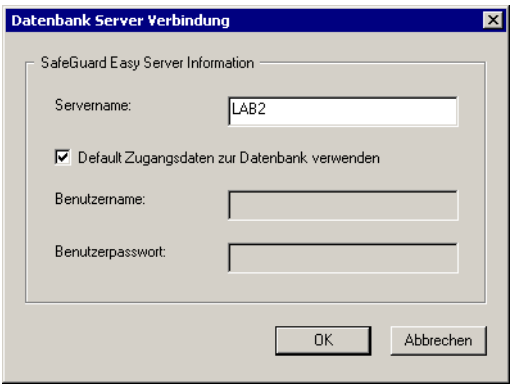


8. Registrierungsrequest starten über das **Menü Extras / Push Request durchführen**.

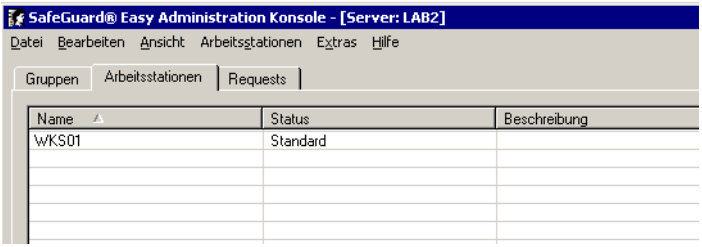


9. Der SafeGuard Easy Client, seine Warteschleife (Queue) und andere Datenbankabhängigkeiten werden aus der alten Datenbank entfernt.

10. Die Administrationskonsole starten und zum neuen SafeGuard Easy Server verbinden.



11. Der umregistrierte SafeGuard Easy Client erscheint in der Administrationskonsole.



31.6 Gruppen definieren

Die Administrationskonsole verwaltet die einzelnen SafeGuard Easy Clients, die sich am SafeGuard Easy Server registriert haben. In großen Organisationen ist es jedoch oft sinnvoll, die SafeGuard Easy Clients in Gruppen zusammenzufassen um etwa an eine große Anzahl von PCs Konfigurationseinstellungen zu verteilen. Gruppen gliedern sich bspw. nach Abteilungen oder auch nach identischen SafeGuard Easy Einstellungen. Trotz Gruppenzuordnung sind für Clients zusätzlich eigene Konfigurationen möglich.

Innerhalb der SafeGuard Easy Gruppen gibt es keine Hierarchien, d.h. Gruppe A kann nicht Gruppe B enthalten, Gruppe C hat nicht mehr Rechte als Gruppe D etc. Jedoch kann jeder SafeGuard Easy Client Mitglied in beliebig vielen Gruppen sein.

Die Gruppierung von Clients ist in großen Organisationen sehr zeitaufwendig. Im Rahmen einer vorkonfigurierten Installation weist ein SafeGuard Easy Parameter Clients während der Installation automatisch einer oder mehreren Gruppen zuzuweisen (siehe Parameter `Groups` unter 'SafeGuard Easy Parameter').

Die SafeGuard Easy Gruppen arbeiten unabhängig von existierenden Windows-Benutzergruppen!

31.6.1 Gruppen erstellen / löschen

Zum Erstellen einer Gruppe wechseln Sie in die Registerkarte **Gruppen** und wählen Sie **Gruppe erstellen**. Im erscheinenden Dialog geben Sie einen Gruppennamen ein, der nach Bestätigen in der Registerkarte Gruppen aufgelistet wird.

Nicht mehr benötigte Gruppen werden über das **Menü Gruppen / Gruppe löschen** entfernt.

Trotz Löschen bleiben Requests, die für Gruppen abgeschickt wurden, in der Warteschleife bestehen und werden ausgeführt.

31.6.2 SafeGuard Easy Client einer Gruppe zuweisen / aus einer Gruppe entfernen

Sollen SafeGuard Easy Clients auf Gruppenbasis administriert werden, muss ihnen ein bereits existierender Gruppenname zugeordnet werden.

1. In die **Registerkarte Arbeitsstation** wechseln.
2. Einen SafeGuard Easy Client markieren
3. Im **Menü Arbeitsstation** den Befehl **Zu Gruppen zuweisen** aufrufen.
4. Gruppe markieren und Angabe bestätigen.

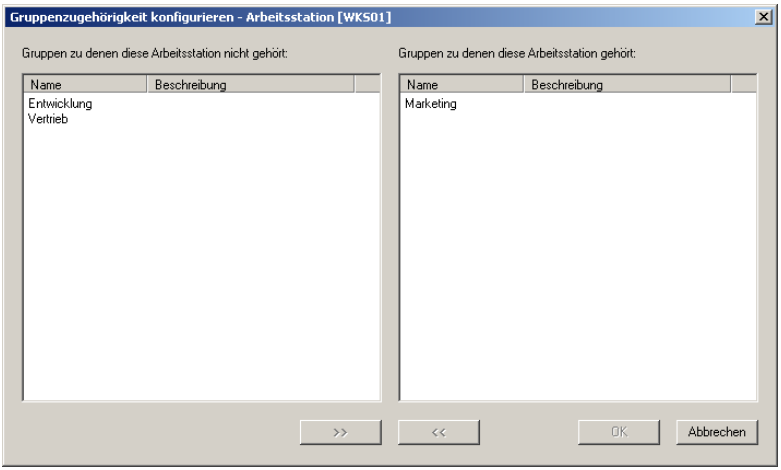
Entfernt wird ein Client über **das Menü Arbeitsstation / Aus Gruppe entfernen**.

Die Gruppenzusammensetzung sollte nicht geändert werden, solange noch auszuführende Requests anstehen!

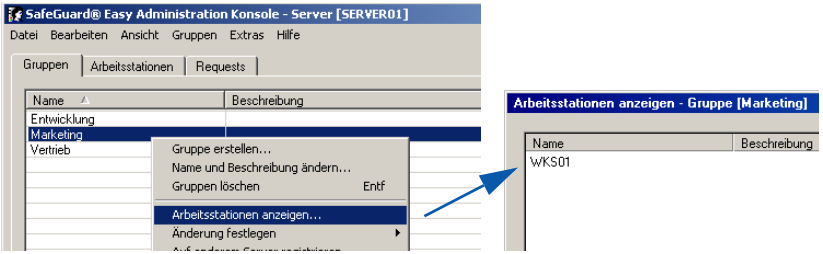
31.6.3 Gruppenzugehörigkeit

Administratoren müssen sich einen schnellen Überblick über die Gruppenzusammensetzungen verschaffen können, um sicherzustellen, dass Clients immer mit korrekten Daten versorgt werden.
Die Administrationskonsole liefert diese Daten über

- das Menü **Arbeitsstationen / Gruppenzugehörigkeit:**
  Fragt die Gruppenzugehörigkeit eines SafeGuard Easy Clients ab. Über die Pfeiltasten gibt es die Möglichkeit, die Gruppenzugehörigkeit zu ändern.



- das Menü **Gruppen / Arbeitsstationen anzeigen:**
  Listet die Mitglieder einer Gruppe auf



31.6.4 Gruppennamen ändern

Zum Ändern eines Gruppennamens, klicken Sie auf **Name und Beschreibung ändern** im **Menü Gruppen**. Geben Sie den neuen Gruppennamen ein und bestätigen Sie ihn mit OK.

31.6.5 Gruppe löschen

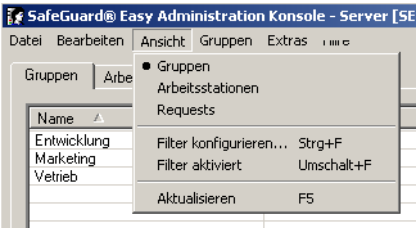
Zum Löschen einer Gruppe, klicken Sie auf **Gruppen löschen** im **Menü Gruppen**.

31.7 Filter definieren

Die Administrationskonsole verfügt über einen Filtermechanismus, mit dem der Administrator passgenau bestimmen kann, welche SafeGuard Easy Clients, Gruppen oder Requests er am Bildschirm sieht. Dieses Verfahren bietet sich an bei einer großen Anzahl an verwaltbaren Objekten, um die Administration zu erleichtern und die Übersichtlichkeit zu bewahren.

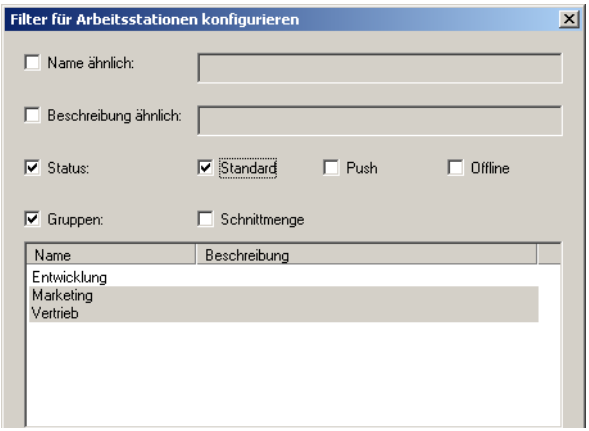
Die Filterdefinition wird über das **Menü Ansicht** der jeweiligen Registerkarte aufgerufen und erfolgt in zwei Schritten:

- Filter konfigurieren
- Filter aktivieren



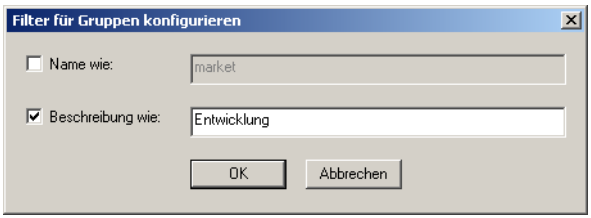
31.7.1 Filter konfigurieren

Arbeitsstationen können anhand einer Vielzahl von Regeln sichtbar/unsichtbar gemacht werden. Eine erweiterte Option erlaubt sogar, die Schnittmenge markierter Gruppen als Regel zu definieren (d.h. Arbeitsstationen werden nur angezeigt, wenn sie Mitglied von Gruppe A und Gruppe B sind).

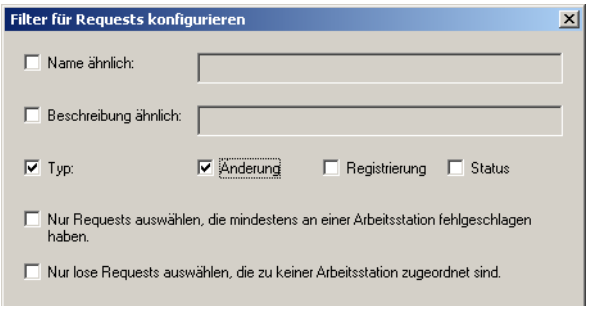


Ansicht für Arbeitsstationen

Für **Gruppen und Requests** ist das Filtern nach Name und Beschreibung möglich. Für Requests gibt es noch zusätzlich die Möglichkeit, den Request-Typ und fehlgeschlagene bzw. nicht zugeordnete Requests anzeigen zu lassen.



Ansicht für Gruppen

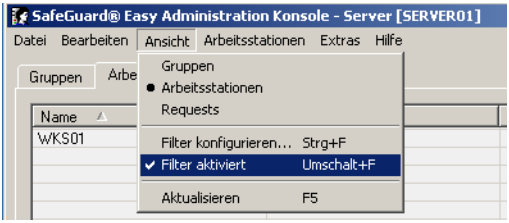


Ansicht für Requests

Sie können zur Definition in den Feldern „Name“ und „Beschreibung“ auch Wildcards verwenden. Als Wildcardzeichen wird nur das *-Symbol akzeptiert. Dies bedeutet, dass an der Position mit dem Zeichentyp „*“ mehrere beliebige Zeichen im Namen / in der Beschreibung enthalten sein können.

Allgemein gilt folgende Regel: Angezeigt werden ausschließlich Arbeitsstationen / Gruppen / Requests, für die jede der gewählten Eigenschaften zutrifft.

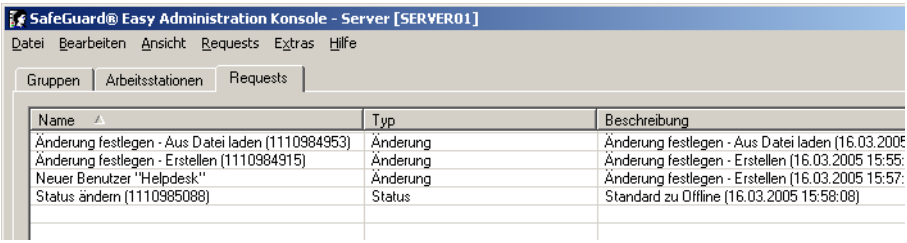
31.7.2 Filter aktivieren



Der Filter entfaltet seine Wirkung erst, wenn er aktiviert wurde. Dass im Filtermodus gearbeitet wird, erkennt der Benutzer an der geänderten Farbe der Arbeitsoberfläche der Administrationskonsole. Der weiße Standard-Hintergrund wechselt dann beispielsweise zu blau.

31.8 Requests und Warteschleifen

Requests enthalten Konfigurationsupdates für SafeGuard Easy Clients. Der SafeGuard Easy Client holt diese Updates vom SafeGuard Easy Server ab, sobald beide miteinander kommunizieren. Findet ein SafeGuard Easy Client aktuelle Änderungen, führt er sie gemäß der Reihenfolge aus, in der sie dem Client über die Administrationskonsole zugewiesen wurden. Einmal erstellte Requests sind beliebig oft für verschiedene Gruppen/Arbeitsstationen anwendbar. Alle abgeschickten Requests werden - unabhängig von ihrem Status - in der Warteschleife unter der Registerkarte „Requests“ gesammelt.



Ein Request entspricht prinzipiell der Funktion einer Konfigurationsdatei (siehe ’Neue Konfigurationsdatei erstellen’) und führt Änderungen an bereits bestehenden SafeGuard Easy Einstellungen eines Clients durch. Eine Änderung kann ein kleiner Eingriff in die Konfiguration des SafeGuard Easy Client sein, aber auch die Deinstallation von SafeGuard Easy ist möglich. Einzig Installationen sind per Request nicht vorgesehen. Im Bedarfsfall integrieren Requests auch bereits vorhandene Konfigurationsdateien.

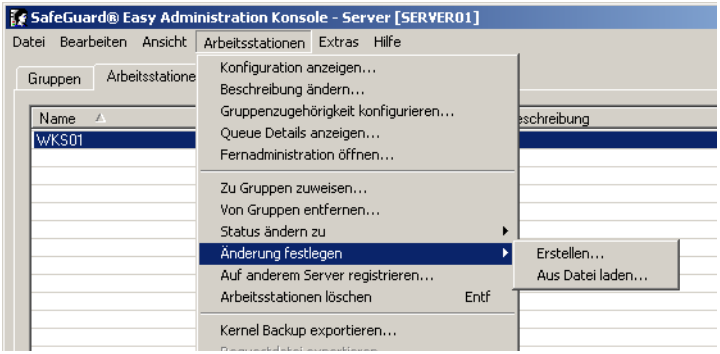
Erfolg/Misserfolg eines Requests werden sofort an den Server übermittelt, so dass der Administrator immer genau über den aktuellen Stand informiert ist. Erfolgreich ausgeführt wird ein Request nur, wenn die Erstellerinformationen (SafeGuard Easy Benutzer-ID und Passwort) mit denen eines SafeGuard Easy Benutzers auf dem SafeGuard Easy Client übereinstimmen. Zusätzlich muss das Rechteprofil des Erstellers es ermöglichen, dass die angegebenen Änderungen auf dem Client ausgeführt werden dürfen.

Requests werden gemäß ihres Erstellungsdatums in eine Server-**Warteschleife** eingereiht und warten dort auf Abholung durch den Client. Clients holen immer zuerst den Request mit dem ältesten Erstellungsdatum ab.

31.8.1 Requests erstellen

Neue Requests können für einzelne SafeGuard Easy Clients oder für Gruppen erstellt werden. Kommt ein SafeGuard Easy Client in mehreren Gruppen vor, wird der Request trotzdem nur einmal ausgeführt.

Neue Request werden über den Befehl **Änderung festlegen** erzeugt, der sowohl im **Menü Arbeitsstation** als auch im **Menü Gruppen** zu finden ist.

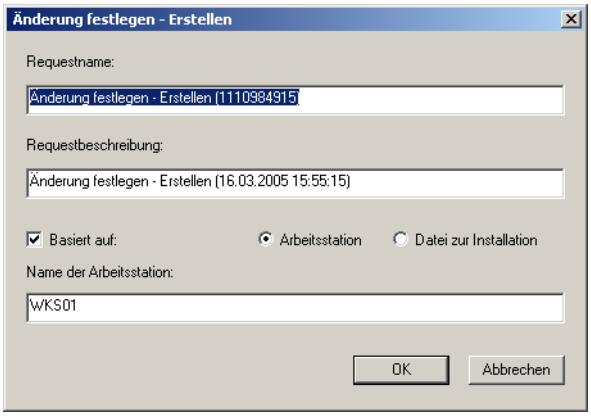


Nach dem Aufruf von **Änderung festlegen** wählt der Benutzer zwischen

- **Erstellen**
  Erzeugt einen neuen Request
- **Aus Datei laden**
  Verwendet bestehende Konfigurationsdatei als Request.

31.8.2 Neuen Request erstellen

Über **Arbeitsstationen (Gruppen) / Änderungen festlegen / Erstellen** wird ein Dialog aufgerufen, in dem man eine Vorauswahl trifft, ob ein Request mit Vorlage (einer sogenannten Basiskonfiguration) erstellt oder ob darauf verzichtet wird.



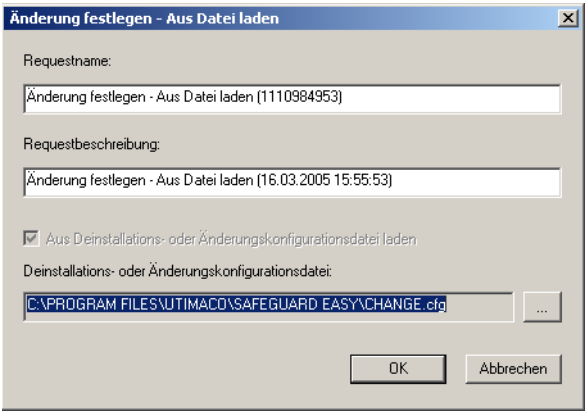
Eine Vorlage zu laden bietet sich an, wenn sie Einstellungen enthält, die sich nur geringfügig vom geplanten Request unterscheiden. Sie erleichtert die Arbeit des Administrators, da wiederholtes Eintippen/Anklicken von Optionen entfällt. Der Request basiert dann entweder auf den Einstellungen eines am SafeGuard Easy Server registrierten Clients (einzutippen ist dann etwa „WKS-1“), oder auf einer Konfigurationsdatei mit dem Attribut „Installieren“. Mit diesem Mechanismus ist es u.a. möglich, Einstellungen von einer Maschine zur anderen zu kopieren.

Ohne Vorlage wird ein neuer Request erstellt, der seine Einstellungen weder aus einer Konfigurationsdatei noch von einer Arbeitsstation bezieht.

Dem Bestätigen der Dialog-Einträge folgt der Start des Konfigurationsdateiassistenten (siehe 'Konfigurationsdateiassistent'). Erkennt der Konfigurationsdateiassistent eine Installationsdatei als Basis, verlangt er eine Authentisierung bevor alle Daten angezeigt werden.

31.8.3 Bestehende Konfigurationsdatei als Request verwenden

Über **Arbeitsstationen (Gruppen) / Änderungen festlegen / Aus Datei Laden** kann einem Request auch direkt eine bestehende Konfigurationsdatei mitgegeben werden, die SafeGuard Easy von einem SafeGuard Easy Client deinstalliert oder nur Änderungen vornimmt. Voraussetzung dafür ist, dass diese Datei zuvor mit dem Konfigurationsdateiassistenten erstellt wurde.



Für die Arbeit mit bestehenden Konfigurationsdateien spricht ihre „Lebensdauer“. Requests ohne mitgegebener Konfigurationsdatei sind nach Fertigstellung nicht als eigene Datei verfügbar, sondern als Verknüpfung in der SafeGuard Easy Datenbank abgelegt. Einmal erfolgreich ausgeführt lassen sich ihre Einstellungen im Nachhinein nicht mehr editieren bzw. anderen Arbeitsstationen zuweisen!

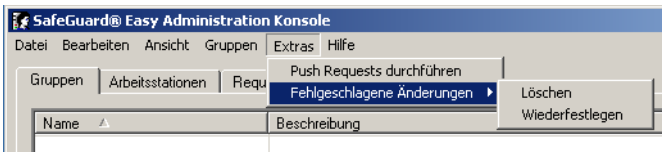
31.8.4 Fehlgeschlagene Requests

Requests können fehlschlagen,

- wenn die Authentisierung des Request-Erstellers auf dem SafeGuard Easy Client fehl schlägt.
- wenn das Rechteprofil des Request-Erstellers nicht erlaubt, eine im Request eingetragene Änderung am SafeGuard Easy Client durchzuführen. Wenn bereits eine Einstellung im Request nicht ausgeführt werden kann, wird der gesamte Request nicht ausgeführt!
- wenn aus bestimmten Gründen keine Netzwerkverbindung zwischen SafeGuard Easy Client und SafeGuard Easy Server besteht (In dringenden Fällen Rückgriff auf das Verfahren mit Offline-Clients empfohlen).
- wenn Eintragungen im Request nicht mit den SafeGuard Easy Einstellungen auf dem Client übereinstimmen (z.B. Angabe eines falschen SafeGuard Easy Passworts im Request für einen SafeGuard Easy Benutzer).

Ein fehlgeschlagener Auftrag stoppt das Abarbeiten weiterer Aufträge in der Warteschleife (u.a. auch das Exportieren von Requestdateien für Offline Clients).

Sobald der fehlgeschlagene Auftrag aus der Warteschleife entfernt oder neu eingereiht wurde (Menü Extras / Fehlgeschlagene Änderungen), werden alle anstehenden Requests wieder ausgeführt.



31.8.5 Requestnamen ändern

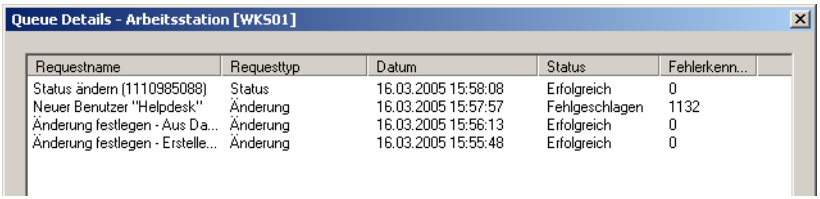
Um einem in der Registerkarte „Requests“ angezeigten Request einen neuen Namen und Beschreibung zu geben, öffnen Sie im **Menü Requests** den Befehl **Beschreibung ändern**. Die geänderten Einträge werden sofort übernommen.

31.8.6 Request löschen

Solange ein Request noch nicht erfolgreich ausgeführt wurde, können „ungewollte“ Änderungen wieder rückgängig gemacht werden. Zu diesem Zweck muss der Request aus Warteschleife herausgenommen werden. Wählen Sie im **Menü Requests / Request löschen**, wird ein markierter Request gelöscht und aus der Warteschleife entfernt.

31.8.7 Warteschleife anzeigen

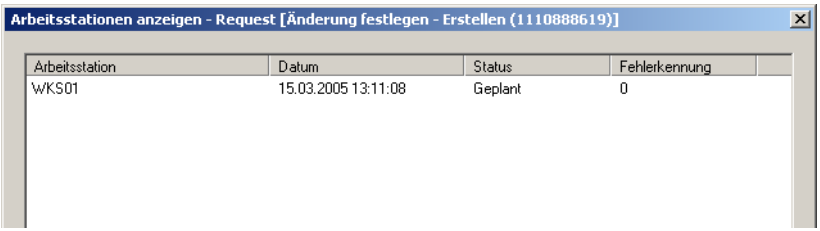
In der allgemeinen Warteschleife (**Menü Arbeitsstation / Queue details**) findet man alle Requests, die für SafeGuard Easy Clients bestimmt sind, deren aktuellen Status (erfolgreich ausgeführt, fehlgeschlagen...) sowie Zeitangaben darüber, wann der Request erstellt wurde.



HINWEIS:

Die Schaltfläche [Löschen] ist aktiv, wenn keiner der selektierten Queue-Einträge auf „Wartend“ steht.

Die Request-spezifische Warteschleife (**Menü Requests / Arbeitsstationen**) listet auf, mit welchen Arbeitsstationen ein markierter Request verbunden ist.



Die Aufträge einer Warteschleife können folgende Eigenschaften besitzen:

- **Erfolgreich:** Der Request wurde auf dem SafeGuard Easy Client ausgeführt und der Server hat eine Benachrichtigung über den erfolgreichen Abschluss erhalten.
- **Fehlgeschlagen:** Der Request wurde ausgeführt, aber es trat ein Fehler während der Ausführung auf und der Server wurde benachrichtigt. Die Bedeutung der angezeigten Nummer kann im Kapitel „Fehlermeldungen“ nachgeschlagen werden.
- **Wartend:** Der Request wurde zum SafeGuard Easy Client geschickt, es ist aber noch keine Nachricht über eine erfolgreiche/ fehlgeschlagene Ausführung am Server eingetroffen.
- **Geplant:** Der Request wartet darauf, zum SafeGuard Easy Client geschickt zu werden. Dieser Zustand tritt ein, sobald der SafeGuard Easy Client den Server kontaktiert oder wenn die Warteschleife in den Push-Modus versetzt wird.

31.9 Status eines SafeGuard Easy Clients

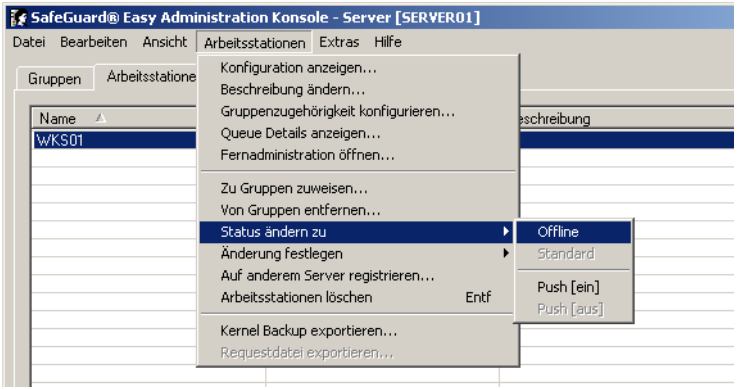
Der Status einer Arbeitsstation bezeichnet die Art der Verbindung, die zwischen SafeGuard Easy Server und SafeGuard Easy Client besteht. Überdies bestimmt der Status, wie die Arbeitstations-Queue vom SafeGuard Easy Server abgearbeitet wird.

Arbeitsstationen können verschiedene Status annehmen, nämlich

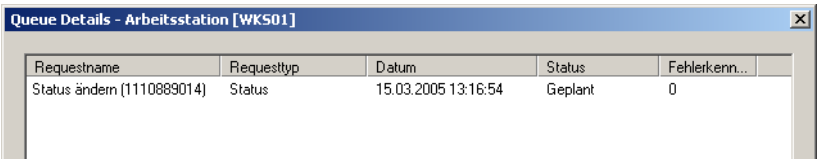
- Standard (Online)
- Offline
- Push ein
- Push aus

Die Status (Standard/Online und Offline) zeigen die Art der Verbindung, die zwischen SafeGuard Easy Server und SafeGuard Easy Client besteht, und somit bestimmen sie auch das Verhalten der Kommunikation zwischen SafeGuard Easy Server und SafeGuard Easy Client. „Push ein“ und „Push aus“ lassen sich mit den anderen beiden Status (Standard/Online und Offline) kombinieren. Arbeitsstationen mit dem Attribut „Push (ein)“ markieren die Arbeitsstationen, deren Queues nach Ausführen eines Kommandos in der Administrationskonsole vom SafeGuard Easy Server sofort abgearbeitet werden sollen.

Die Statusänderung erfolgt über das **Menü Arbeitsstation / Status ändern zu**.



Sobald der Status (auf Standard oder Offline) eines SafeGuard Easy Clients geändert wird, reiht SafeGuard Easy einen „Status-Request“ in die Warteschleife ein.



31.9.1 Status „Standard (Online)“

Jeder Client besitzt nach dem Austausch der Kommunikationsinformationen (Schlüsselpaar, GUID-Erzeugung, Zuweisung des SafeGuard Easy Servernamens) und der anschließenden Erstregistrierung am Server den Status „Standard“. Clients mit dem Attribut „Standard“ sind PCs, die regelmäßig Kontakt mit dem Netzwerk aufnehmen (z.B. stationäre PCs im Bürogebäude). Diese SafeGuard Easy Clients suchen immer von sich aus Kontakt mit dem Server und holen bei jeder Kontaktaufnahme die für sie bestimmten Requests ab, zuerst beim Start des SafeGuard Easy Clients und dann alle 6 Stunden.

31.9.2 Status „Offline“

Bei Offline Clients handelt sich um PCs, von denen man im Voraus weiß, dass sie nie mit dem Netzwerk oder dem SafeGuard Easy Server verbunden sind (z.B. Notebooks von Außendienstmitarbeitern), aber dennoch zentral verwaltet werden sollen. Die Installation wird für solche PCs wie gewohnt mit Erstregistrierung am SafeGuard Easy Server durchgeführt. In der Administrationskonsole schaltet der Administrator den Status des betreffenden Clients dann auf „Offline“. Das tut er nur, wenn er weiß, dass dieser nicht von sich aus versuchen wird, das Netz zu kontaktieren. Fehlgeschlagene Anfragen vom Client an den Server o.ä. weisen einen Client *nicht* als „Offline“ aus.

Der „Offline“ Status kann einem Client bereits bei der Installation zugewiesen werden, indem als Servername „.OFFLINE“ eingetragen wird.

Der „Offline“-Status hat auch Auswirkungen auf die Handhabung von Requests, die für den Offline geschalteten PC erstellt und auf diesem ausgeführt werden sollen. Erstellt der Administrator einen (oder mehrere) Requests für den Client, werden diese in die Warteschleife eingereiht, warten aber vergeblich auf Abholung durch den SafeGuard Easy Client, da keine Verbindung zum SafeGuard Easy Server besteht.

Damit die Änderungen trotz fehlender Client-Server-Verbindung übertragen werden, exportiert eine Funktion der Administrationskonsole alle, für einen Offline-Client geltenden Requests in eine Datei. Diese Datei schickt der Administrator per Mail an den Benutzer des Offline Clients. Dieser importiert die Datei mit Hilfe eines von SafeGuard Easy mitgelieferten Tools. Sobald Requests in eine Request-Datei gespeichert werden, erhalten sie die Eigenschaft „Wartend“ in der Server-Warteschleife. Dies verhindert, dass sie späteren Request-Dateien hinzugefügt werden. Sobald die Request-Datei importiert wurde, werden die Requests in der vorgeschriebenen Reihenfolge auf dem Offline-PC abgearbeitet.

Ohne Kontakt zum Offline-Client weiß der Administrator nicht, ob die Änderungen erfolgreich ausgeführt wurden oder fehlgeschlagen sind. Die fehlenden Informationen liefert ihm eine Report-Datei, die nach Ausführung der Request-Datei erzeugt wird. Diese Datei ist an den Administrator zu übermitteln und in die Administrationskonsole zu importieren (eine entsprechende Import-Funktion steht dort zur Verfügung).

Nach dem Import sieht der Administrator, ob die Konfigurationsänderungen erfolgreich waren, indem er die Eigenschaften des Offline-Clients aufruft.

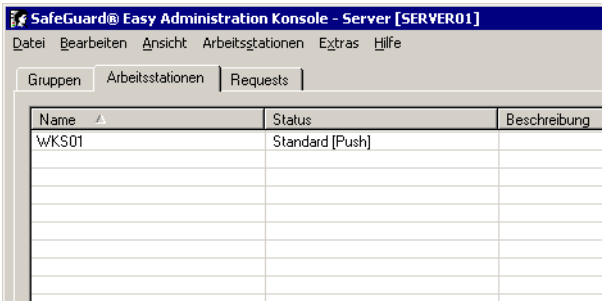
Ein Client kann nur vom Offline- in den Standardmodus wechseln, wenn er mit der die Option „Server-Anbindung“ installiert und der SafeGuard Easy Servername mitgegeben wird.

Das Austauschen von Request-/Report-Dateien ist nicht nur auf Offline-Clients beschränkt. Fällt etwa die Netzwerkverbindung zwischen SafeGuard Easy Clients und SafeGuard Easy Server aus, können Konfigurationsänderungen den nicht erreichbaren Clients mit diesem Verfahren mitgeteilt werden, bis die Clients wieder zentral administrierbar sind.

31.9.3 Status „Push [ein]“

Ein SafeGuard Easy Client kann gezwungen werden, seine Einstellungen vor allen anderen Clients mit dem Server zu synchronisieren. Dies kann eintreffen, wenn ein Benutzer einen Konfigurationswunsch hat oder der Administrator sofortige Änderungen auf den Client überspielen muss (Mitarbeiter verlässt das Unternehmen und der Zugriff auf den Client muss gesperrt werden).

Damit der SafeGuard Easy Server weiß, welcher SafeGuard Easy Client gemeint ist, erhält der SafeGuard Easy Client über das Menü Arbeitsstationen / Status ändern zu / Push [ein] das Attribut „Push“, z.B. „Standard [Push]“.

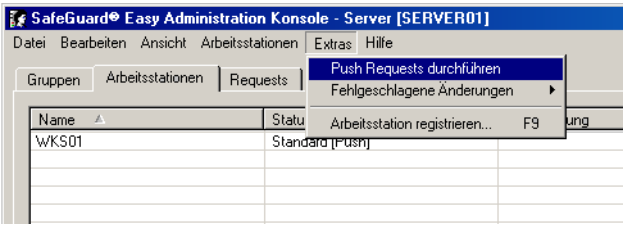


Das „Push“-Attribut eines Clients weckt nach Ausführen des Kommandos „Push Requests sofort anwenden“ aus dem Menü Extras den Server, der sich in der Regel passiv verhält und auf die Anfragen der Clients wartet. Der SafeGuard Easy Server versucht von sich aus, einmal den Client mit dem Attribut „Push“ zu kontaktieren und alle in der Warteschleife befindlichen Aufträge mit der Eigenschaft „Geplant“ für diesen Client abzuarbeiten bis die Warteschleife leer ist oder ein Auftrag fehl schlägt. In beiden Fällen fällt der Server wieder in den passiven (normalen) Zustand zurück und behält diesen bis ihn der Administrator erneut „pusht“. Auch die Clients erhalten dann automatisch wieder den Status „Standard“.

Auch das Attribut „Push“ wird dabei automatisch wieder entfernt.

Der Push-Mechanismus ist ein Kompromiss aus Netzwerklast und Sicherheit.

Wenn der Push-Modus nicht sofort ausgeführt werden soll, kann die Kontaktaufnahme des SafeGuard Easy Servers mit Clients im nachhinein über das **Menü Extras / Push Requests durchführen** angestoßen werden.



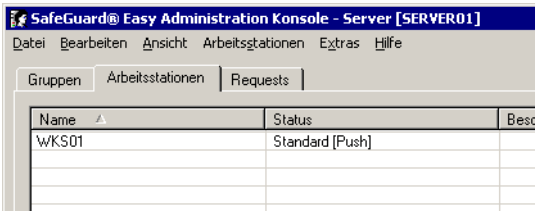
31.9.4 Status „Push [aus]“

Über das **Menü Arbeitsstationen / Status ändern zu / Push [aus]** entfernt SafeGuard Easy das Push-Attribut vom SafeGuard Easy Client.

31.9.5 SafeGuard Easy Client in den OFFLINE Modus schalten

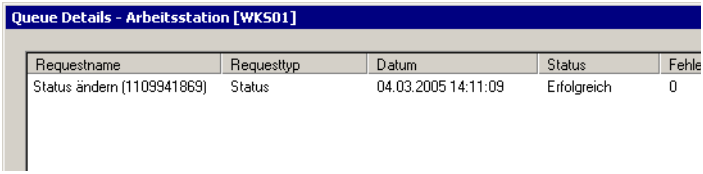
1. **Menü Arbeitsstationen / Status ändern zu** aufrufen.

   Status setzen auf
   a) Offline
   b) Push [ein]

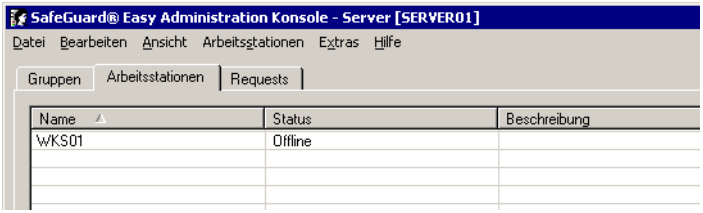


2. Soll der SafeGuard Easy Client sofort in den OFFLINE Modus geschaltet werden, den folgenden Dialog mit [JA] beantworten.

3. In der Warteschleife des SafeGuard Easy Clients wird ein Request zur Statusänderung erzeugt, der das Attribut „Erfolgreich“ erhält.

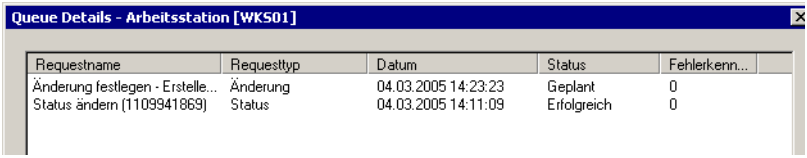


4. Der SafeGuard Easy Client besitzt nun den Status „Offline“.

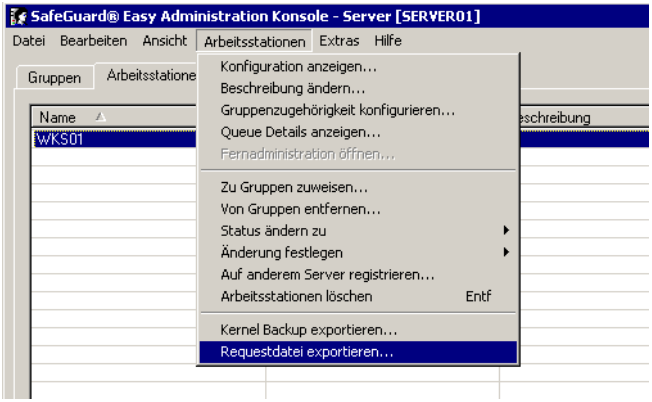


31.9.6 Konfigurationsupdates für Offline Clients in der Administrationskonsole erzeugen

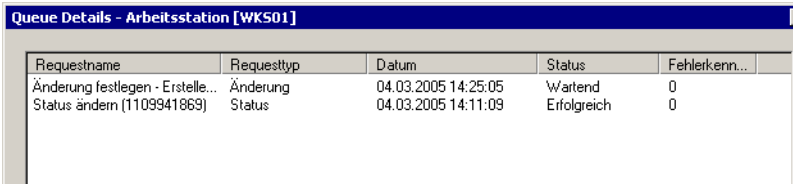
1. Der SafeGuard Easy Administrator erzeugt über das Menü **Arbeitsstationen/Änderung festlegen** ein Konfigurationsupdate („Änderungs-Request“). In der Warteschleife wird der Request auf „Geplant“ gesetzt.



2. Der SafeGuard Easy Administrator exportiert den Request in eine „Request-Datei“ (Dateierweiterung .REQ) über das Menü **Arbeitsstation / Request-Datei exportieren**.

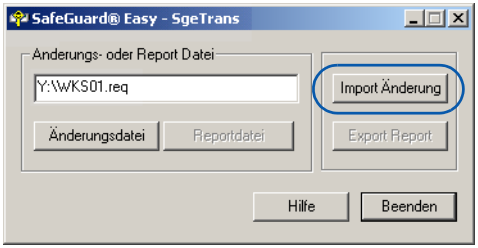


3. Sobald eine Request-Datei erstellt ist, wechselt der Status des Request in der Warteschleife auf „Wartend“.



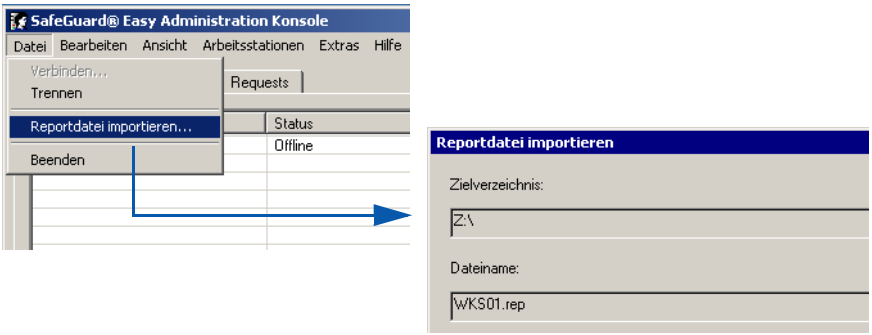
4. Der SafeGuard Easy Administrator schickt die Request-Datei z.B. per Mail an den Benutzer des Offline-Clients.

5. Der Benutzer des Offline-Client importiert die Request-Datei mit SGETrans (siehe auch ’Konfigurationsupdate auf Offline Client einspielen mit SGETRANS’).

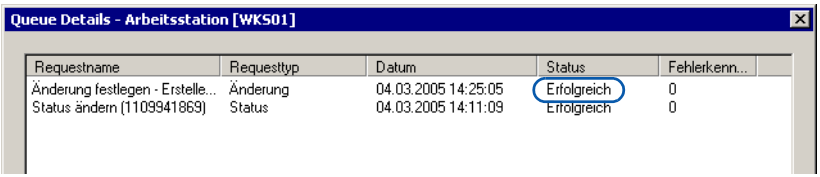


6. SafeGuard Easy teilt dem Benutzer des Offline-Clients mit, ob die Änderungsdatei erfolgreich ausgeführt wurde.
Gleichzeitig wird auf dem Offline-Client ein „Report-Datei“ (Dateierweiterung .REP) erzeugt, die der Benutzer an den SafeGuard Easy Administrator schickt.

7. Der SafeGuard Easy Administrator importiert die Report-Datei in die Administrationskonsole über das **Menü Datei / Report-Datei importieren**.

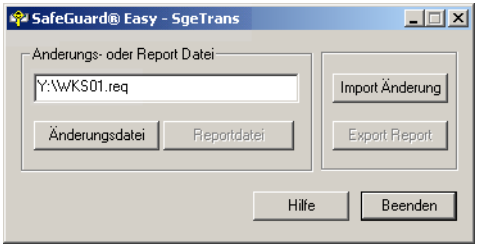


8. Über die Warteschleife (oder die Eigenschaftenseite der Arbeitsstation) sieht der SafeGuard Easy Administrator, ob die Änderungen erfolgreich ausgeführt wurden.



31.9.7 Konfigurationsupdate auf Offline Client einspielen mit SGETRANS

Das Programm SGETrans dient als Schnittstelle für den Austausch von Request und Report-Dateien bei der Arbeit mit Offline-Clients. SGETrans ist im SafeGuard Easy-Verzeichnis nur vorhanden, wenn bei der Client-Installation die Option „Server Anbindung“ gewählt wurde.



- **Änderungsdatei**
  Lädt die Request-Datei, die der Benutzer vom Administrator z.B. per Mail zugesandt bekommt.
- **Import Änderung**
  Speichert die Einstellungen der Request-Datei auf dem Benutzer-PC.
- **Report-Datei**
  Definiert einen Dateinamen für die Report-Datei.
- **Export Report**
  Speichert die Report-Datei, die der Benutzer an den Administrator sendet.

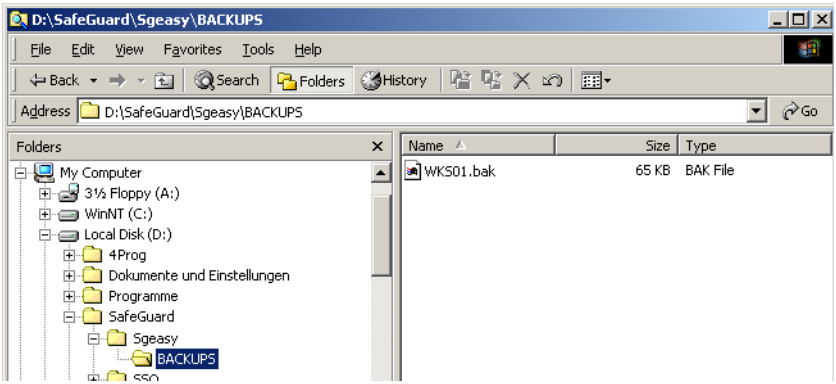
31.10 Systemkern automatisch sichern

Der Systemkern hält die für die Authentisierung am Rechner erforderlichen Funktionen, die für den Start eines Betriebssystems notwendigen Treiber sowie alle Systemeinstellungen eines SafeGuard Easy Clients. Eine aktuelle Sicherung ist besonders in Notfallsituationen gefragt, wenn der Systemkern eines SafeGuard Easy Clients beschädigt ist und Benutzer sich nicht mehr ans System anmelden können. In solchen Fällen braucht man einen intakten Systemkern der betreffenden Arbeitsstation, um den Urzustand wiederherzustellen und das System lauffähig zu machen (siehe 'Notfallmedien erstellen und Systemkern sichern').

Die automatische Systemkernsicherung enthebt den Administrator der Aufgabe, Benutzer an die notwendigen Sicherungen zu erinnern oder diese selbst durchzuführen. Diese Aufgabe übernimmt im Rahmen der zentralen Administration ein Autobackup-Mechanismus. Er veranlasst den SafeGuard Easy Client nach einer erfolgreichen Registrierung eine Systemkernsicherung an den SafeGuard Easy Server zu senden.
Auch nach Eingriffen in die SafeGuard Easy Konfiguration (z.B. über ausgeführte Konfigurationsdateien) erzeugt der SafeGuard Easy Client die Sicherung, sendet sie an den Server und überschreibt die alten Daten. Der Autobackup garantiert, dass der Administrator in Notfallsituationen unabhängig ist von vorhandenen/nicht vorhandenen Benutzersicherungen.

31.10.1 Systemkern eines SafeGuard Easy Clients im Verzeichnis BACKUPS ablegen

In der Grundeinstellung legt SafeGuard Easy den gesicherten Systemkern eines SafeGuard Easy Clients in das SafeGuard Easy Verzeichnis der Maschine, auf der die SafeGuard Easy Datenbank liegt (i.d.R. der SafeGuard Easy Server). Dort wird eigens ein \BACKUPS Verzeichnis erzeugt, in das die Systemkerne kopiert werden. Die Zuordnung der Sicherungen zu den Arbeitsstationen ist sehr einfach: Der Dateiname setzt sich aus dem Namen der registrierten Arbeitsstation und der Erweiterung .BAK zusammen.



31.10.2 Neues Backup-Verzeichnis angeben

Mit dem Registry Eintrag **BackupDirectory** in

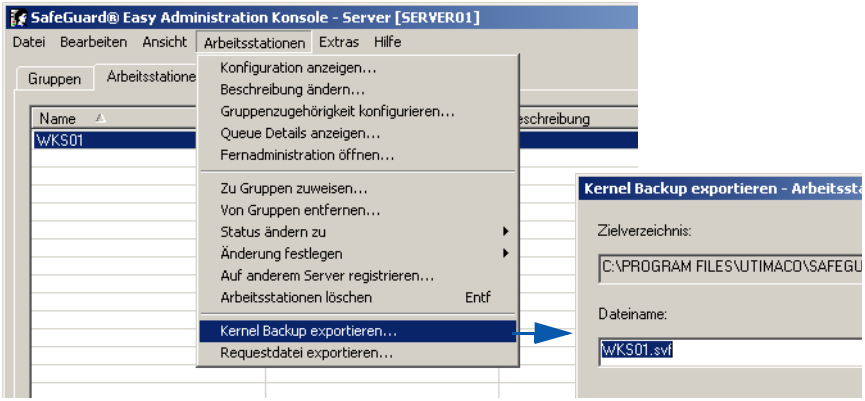
HKEY_LOCAL_MACHINE
SOFTWARE
Utimaco
Sgeasy

kann ein anderes Backup-Verzeichnis definiert werden. Die Einstellung wird erst nach einem Neustart wirksam. Grundsätzlich ist es möglich, sowohl lokale Laufwerkspfade als auch UNC Pfade anzugeben. Bei UNC Pfaden muss sichergestellt sein, dass ausreichende Berechtigungen („Ändern“) eingerichtet werden.

Der Registry-Eintrag muss auf dem PC gesetzt werden, auf dem sich die SafeGuard Easy Datenbank befindet.

31.10.3 Systemkernsicherung exportieren

Die Systemkernsicherungen aller SafeGuard Easy Clients sind auch direkt über die Administrationskonsole exportierbar. Speichern Sie den gesicherten Systemkern über das **Menü Arbeitsstationen/Kernelbackup exportieren** in eine Datei. Zielverzeichnis, Dateinamen und -erweiterung sind dabei frei wählbar.



Geben Sie die Datei an den Benutzer weiter, an dessen PC ein Systemfehler aufgetreten ist. Wie mit Hilfe eines intakten Systemkerns Systemfehler auf Arbeitsstationen behoben werden können, erfahren Sie im Kapitel 'Notfallmedien erstellen und Systemkern sichern'.

32 Remote Administration

Bei der Remote Administration verbindet sich der Administrator von seinem Arbeitsplatz aus mit genau einem einzigen SafeGuard Easy Client und passt die SafeGuard Easy Konfiguration seinen Wünschen an. Der Administrator hat das Gefühl, als ob er direkt vor dem SafeGuard Easy Client sitzt und lokal die Änderungen vornimmt.

Änderungen über die Remote Administration wirken teilweise unmittelbar auf dem SafeGuard Easy Client, wie etwa beim Anstoßen von Verschlüsselung/Entschlüsselung, andere erfordern einen Neustart des SafeGuard Easy Clients.

Die Remote Administration arbeitet unabhängig von der zentralen Administration und bietet sich für Verwaltungsaufgaben in kleineren Netzwerken an. Sie kann stand-alone oder als integraler Bestandteil der Administrationskonsole verwendet werden und erlaubt dem Administrator folgende Aufgaben:

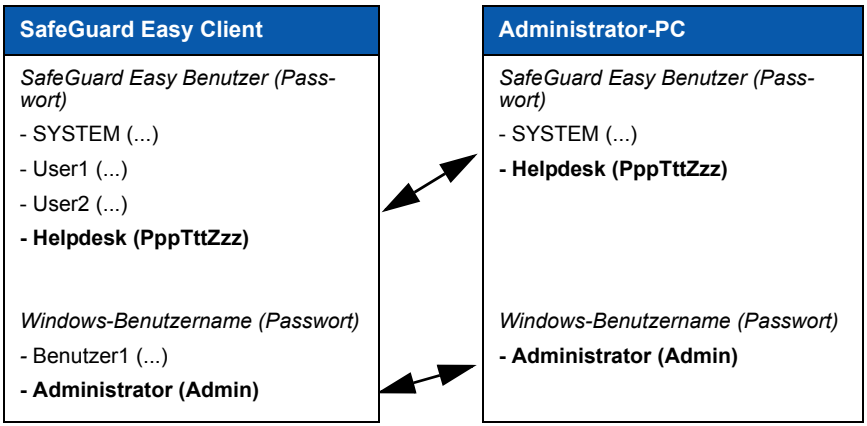
- Verbinden zu einem SafeGuard Easy Client
- Authentisierung an dem SafeGuard Easy Client
- Einstellungen des SafeGuard Easy Clients ändern
- Anzeige von Ver-/Entschlüsselungsprozessen auf SafeGuard Easy Client
- Einstellungen speichern
- Systemkernsicherung des SafeGuard Easy Clients initiieren.

Die Funktionalität der Remote Administration integriert sich in die bekannte SafeGuard Easy Administration und nutzt deren vorhandene Verwaltungsmechanismen.

32.1 Voraussetzungen

Das Betrachten und Editieren von Einstellungen eines SafeGuard Easy Client auf dem Administrator-PC ist nur möglich,

- wenn zwischen Administrator-PC und SafeGuard Easy Client eine Netzwerkverbindung besteht.
- wenn auf dem SafeGuard Easy Client und dem Administrator-PC das Windows-Konto (identischer Benutzername und Passwort) besteht, mit dem sich der Administrator am Administrator-PC angemeldet hat (beim Aufbau der Verbindung erfolgt eine automatische Anmeldung an den SafeGuard Easy Client).
- wenn auf dem SafeGuard Easy Client und dem Administrator-PC mindestens ein identischer SafeGuard Easy Benutzer (samt Passwort) angelegt ist.
- wenn sich der Benutzer des Administrator-PC mit diesen identischen SafeGuard Easy Benutzerinformationen an die SafeGuard Easy Administration mit integrierter Remote Administration anmeldet.



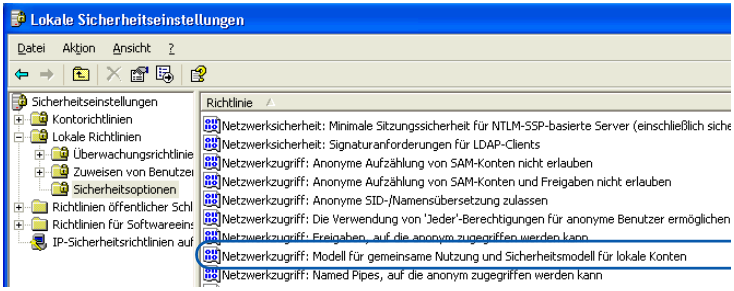
Der SafeGuard Easy Benutzer am Administrator-PC kann nur die Aufgaben ausführen, zu denen er gemäß seinem Benutzerprofil berechtigt ist!

HINWEIS:

Das Betriebssystem Windows XP verlangt folgende Lokale Sicherheitseinstellung auf Client und/oder Administrator-PC:

„Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten = Klassisch - lokale Benutzer authentifizieren sich als Sie selbst“.

Zu den Lokalen Sicherheitseinstellungen gelangen Sie über Systemsteuerung / Verwaltung / Lokale Sicherheitsrichtlinie.

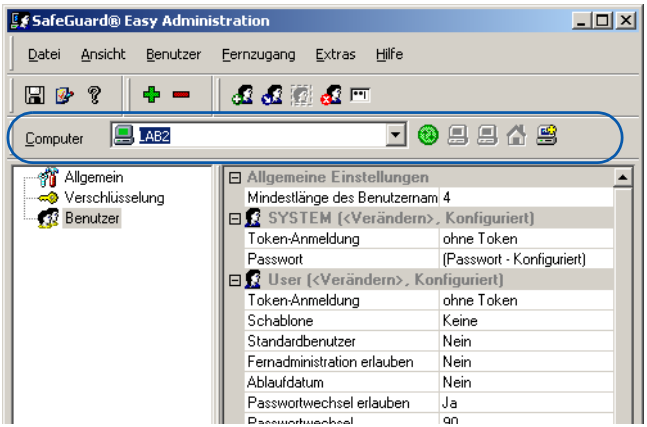


32.2 Installieren der Remote Administration

Zur Fernkonfiguration der SafeGuard Easy Clients ist es notwendig, die Remote Administration auf dem Computer (Administrator-PC) zu installieren, von dem aus Sie die SafeGuard Easy Clients konfigurieren möchten.

Die Installation erfordert diese Schritte:

1. Rufen Sie `Sgeasy.msi` aus dem CD-Verzeichnis \CLIENT auf. Wählen Sie den Installationstyp „Standard“.
2. Rufen Sie `Server.msi` aus dem CD-Verzeichnis \SERVER auf. Wählen Sie die Option „Remote Administration“.
3. Stellen Sie sicher, dass zwischen Administrator-PC und Benutzer-PC eine Netzwerkverbindung besteht.
4. Starten Sie die Remote Administration über **Start / Programme / Utimaco / SafeGuard Easy / Administration**.

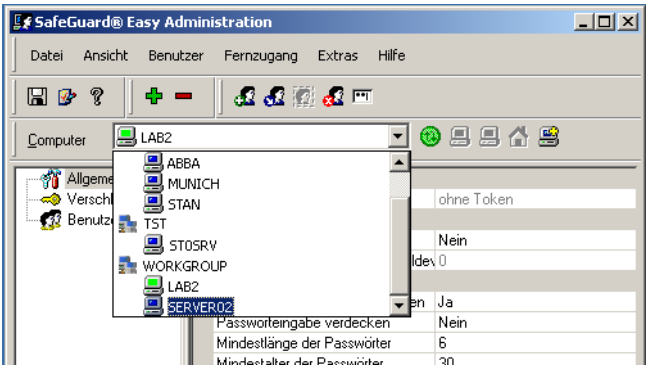


5. Nach der Installation der Remoteverwaltung ist die SafeGuard Easy Administration um diese Funktionen erweitert:
   - Clients über eine Computerliste auswählen
   - Computerliste aktualisieren
   - Verbindung mit dem Client aufbauen / trennen
   - Client-Name manuell eintragen, der nicht in der Computerliste auftaucht.

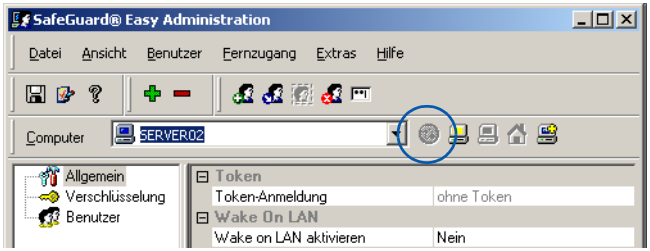
32.3 Verbindung zu einem SafeGuard Easy Client aufbauen

1. Benutzer des Administrator-PCs meldet sich an der SafeGuard Easy Administration an.

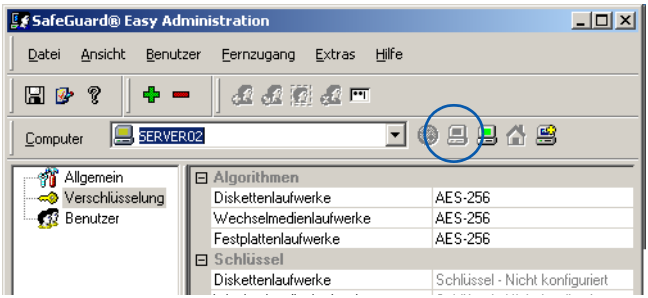
2. Sobald die Computer-Liste aufgeklappt wird, sind die mit dem Netzwerk verbundenen PCs (auch die Domänen) sichtbar. Der grün markierte PC ist dabei der Administrator-PC.



3. Wenn ein Client in der Liste angewählt und anschließend das Symbol mit dem gelb markierten PC gedrückt wird, baut sich eine Verbindung zwischen Administrator-PC und SafeGuard Easy Client auf.



4. Mit Drücken des Symbols mit dem grün markierten PC meldet sich der Benutzer des Administrator-PCs an den SafeGuard Easy Client an (im Beispiel mit „Helpdesk“).



5. Konnte mit diesem SafeGuard Easy-Benutzer keine erfolgreiche Anmeldung durchgeführt werden, wird der Benutzer zur Eingabe gültiger Benutzerdaten aufgefordert.

33 Fehlermeldungen

In diesem Kapitel finden Sie eine Liste aller Fehlermeldungen. Da bei jeder Fehlermeldung von SafeGuard Easy die Fehlernummer angezeigt wird, können Sie den gesuchten Kommentar leicht finden.

Alle Fehlermeldungen haben folgendes Format:

SGEnnnn: <Erklärung des Fehlers>

´SafeGuard Easy´ ist die Produkt-ID von SafeGuard Easy, ´nnnn´ eine vierstellige Fehlernummer.

Für bestimmte SafeGuard Easy-Fehler erhalten Sie zusätzliche Information in der Utimaco-Wissensdatenbank http://www.utimaco.de/myutimaco.

Hier finden Sie ausführliche Informationen zu folgenden SafeGuard Easy-Fehlermeldungen:

0104, 0113, 0400, 0401, 0404, 1048, 1062, 1074, 1089, 1104, 1109, 1121, 1123, 1244, 1254, 1264, 1274, 1306, 1315, 1509, 1602.

Nutzen Sie bitte die Suchfunktion der Wissensdatenbank, um nach Stichworten wie „Fehlermeldungen“, „Error message“ oder der Fehlernummer zu suchen.

Produktspezifische Fehler

0001	Fataler Fehler.
0002	Wiederhole.
0100	Andere Version von [PN] oder Crypton bereits installiert.
0101	Konfigurationsdatei kann nicht gelesen werden.
0102	Ungültige Konfigurationsdatei.
0103	Konfigurationsdatei kann nicht geschrieben werden.
0104	Der momentan installierte Treiber ist nicht konsistent.
0105	Treiber bereits installiert.
0106	Dieses Programm läuft nicht unter &0.
0107	Backup Datei kann nicht geschrieben werden.
0108	Backup Datei kann nicht gelesen werden.
0109	Backup Datei ungültig.
0110	Eine zweite Boot Partition kann nicht erzeugt werden.
0111	Installation auf OS/2 Boot Manager nicht möglich.
0112	Eine frühere Version von [PN] oder C:CRYPT ist bereits installiert.
0113	Letzter Installations-, Deinstallations- oder Updatevorgang nicht beendet.
0114	Nicht genügend zusammenhängenden freien Festplattenspeicher auf der Boot Partition.
0115	Zugriff auf Treiber Boot Partition nicht möglich.
0116	Keine Resource Dateien gefunden.
0117	Resource Datei kann nicht geöffnet werden.
0118	Ungültige oder fehlerhafte Resource Datei.
0119	Algorithmus Modul fehlt.
0120	Kernel Modul fehlt.
0121	PBA Modul fehlt.

0122	*AUTOUSER kann nicht erzeugt werden.
0200	Festplatten Struktur kann nicht analysiert werden.
0201	Festplatten Lesefehler.
0202	Festplatten Schreibfehler.
0203	Ungültige Partitionstabelle auf Festplatte 0.
0204	Inkompatibles ROM BIOS.
0205	Ungültiger Bootsektor.
0206	Volume kann nicht gelockt werden.
0300	Schreibschutzfehler.
0301	Unbekannte Einheit.
0302	Laufwerk &0 nicht bereit.
0303	Unbekannter Befehl.
0304	Daten Checksummenfehler.
0305	Bad request structure length.
0306	Suchfehler.
0307	Unbekannter Medientyp.
0308	Sektor nicht gefunden.
0309	Drucker hat kein Papier mehr.
0310	Schreibfehler.
0311	Lesefehler.
0312	Genereller Fehler.
0320	Nicht genügend Speicherplatz.
0321	Divisionsfehler an Programmadresse &0.
0322	Runtime stack overflow.
0500	Verschlüsselungstreiber nicht installiert.
0501	Inkorrekte Version des Verschlüsselungstreibers.
0502	Kommandozeilenargumente) ungültig.
0503	Kein Schlüssel für die Verschlüsselung definiert.
0999	Unbekannter Fehler.

System API Fehler

1001	Kein Subsystem aktiv.
1002	Unzulässige Änderung einer Systemeinstellung.
1003	Verschlüsselungsalgorithmus fehlt oder ist ungültig.
1004	Interner Fehler im Subsystem entdeckt.
1005	Das Subsystem meldet einen I/O Fehler.
1006	Zugriff auf den Kernel nicht erfolgreich.
1007	Ein Benutzer hat sich bereits an [[FILE-LINK]=SGE_INFO.DLL][[MSGLINK]=102] angemeldet.
1008	Ein ungültiger Benutzer wurde angelegt.
1009	Die Zuweisung definierter Rechte an den Benutzer ist nicht erlaut.
1010	Angelegter Benutzer existiert bereits!
1011	Das vergebene Passwort wurde von diesem Benutzer bereits verwendet.
1012	Das vergebene Passwort gehört zur List der nicht erlaubten Passworte.

Dateifehler

1031	Datei <Name der Datei> kann nicht geöffnet werden.
1032	Datei <Name der Datei> kann nicht geschlossen werden.
1033	Datei <Name der Datei> kann nicht erzeugt werden.
1034	Fehler während Schreibzugriff auf Datei <Name der Datei>.
1035	Fehler während Lesezugriff in Datei <Name der Datei>.
1036	Fehler beim Zugriff auf Datei <Name der Datei>.
1037	Datei <Name der Datei> konnte nicht gefunden werden.
1038	Ungültige Datei oder Pfadname.
1039	Nicht genügend Speicherplatz auf dem Datenträger.
1040	Die Festplattenpartition ist zu stark fragmentiert.

1041	Ungültiges Dateisystem entdeckt.
1042	Unbekanntes Dateisystem entdeckt.
1043	Datei <Name der Datei> existiert bereits.
1044	Korrupte Struktur im Dateisystem entdeckt.
1045	Ungültiger Eintrag im Dateisystem gefunden.
1046	Anforderung nach Partitionsinformationen fehlgeschlagen.
1047	Unbekanntes oder ungültiges Dateisystem entdeckt.
1048	Datei <Name der Datei> konnte nicht kopiert werden.
1049	Datei <Name der Datei> konnte nicht gelöscht werden.
1052	Checksumme der Datei <Name der Datei> fehlerhaft.
1053	Datei <Name der Datei> konnte nicht umbenannt werden.

Installationsfehler

1061	Ungültiges Installationslaufwerk.
1063	SafeGuard Easy ist bereits installiert.
1064	Eine Twinboot Installation ist auf einem System mit mehr als einer Festplatte nicht erlaubt.
1065	Datei Config.sys ist schreibgeschützt.
1066	Eintrag in INI-Datei oder Konfigurationsdatei nicht gefunden.
1067	Auf einem Rechner mit dynamischen Partitionen kann weder ein komplettes noch ein Laufzeit-System von [PN] installiert werden. Nur die Installation von Aministrationswerkzeugen ist auf diesem Rechner erlaubt.
1068	Die Kerneldatei konnte nicht erzeugt werden.
1069	Die Datei Config.sys konnte nicht modifiziert werden.
1070	Die Datei <Name der Datei> konnte nicht kopiert werden.
1071	Kein Zielverzeichnis definiert.
1072	Ein falsches Systemverwalterpasswort wurde angegeben. Wollen Sie es nochmals versuchen?
1073	Kein Systemverwalterpasswort angegeben.

1074	Für den Twin Boot Modus muss das Windows Startlaufwerk auf 'startbar' gesetzt sein.
1075	Das Installationslaufwerk muss für den Twin Boot Modus verschlüsselt werden.
1076	Die Deinstallation ist fehlgeschlagen. Zusätzliche Informationen können Sie der Datei SGEASY.LOG entnehmen.
1077	Die Deinstallation des GINA Systems ist fehlgeschlagen.
1078	Neue Treiber und Systemdienste wurden installiert. Es wird empfohlen, daß Sie jetzt ein neues Backup erzeugen, da die alten Backupdaten nicht für ein Restore verwendet werden können, solange SafeGuard Easy installiert ist!
1079	Die Deinstallation der GINA Clients SGEGINA schlug fehl.
1080	Das Erzeugen eines Menüeintrages schlug fehl.
1081	Das Entfernen eines Menüeintrages schlug fehl.
1082	Eintrag in INI-Datei nicht gefunden.
1083	Die Installation der Cardman API schlug fehl.
1084	Für den Twinboot Modus muss das Kernellaufwerk verschlüsselt sein.%0
1085	Für den Twinboot Modus muss mindestens ein unverschlüsseltes Startlaufwerk definiert sein.
1086	Ein komplettes [PN] System ist noch installiert auf Ihrem Computer auf einer anderen Plattform. Sie müssen dieses System zuerst deinstallieren, bevor Sie das Runtime System des aktuellen Systems deinstallieren können.
1087	Die Installation eines [PN] Systems ist nicht erlaubt.
1088	Eine benötigte PBA Ressourcendatei (.MOD) konnte nicht gefunden werden!
1089	Die Installation von [PN] ist fehlgeschlagen! Folgender Fehler trat auf: Bitte klicken Sie auf OK, um alle bereits installierten Komponenten von [PN] wieder zu entfernen. Danach wird das System automatisch neu gestartet.
1090	Falsche Betriebssystemversion vorgefunden.

1091	Falsche Betriebssystemversion vorgefunden. Das Betriebssystem Windows 95/98/ME ist erforderlich!
1092	Der Deinstallationsvorgang kann nicht gestartet werden, weil eine oder mehrere [PN] Komponenten sind momentan nicht aktiv.
1093	Dieser Prozess kann nicht ausgeführt werden, weil zur Zeit ein Verschlüsselungsprozess läuft. Bitte warten Sie bis alle Verschlüsselungsvorgänge beendet sind und starten Sie dann das Programm erneut.
1094	Die Deinstallation läuft gerade. Administration ist nicht möglich.
1095	Die maximal Anzahl an Festplatten is übertroffen. Die Installation eines [PN] Systems ist nicht erlaubt.
1096	Einige non-DOS Partitionen wurden gefunden, die unter Verwendung des gewählten Installationstyps verschlüsselt werden würden. Wir empfehlen daher, den Installationstyp 'Partitionsweise' auszuwählen.
1097	Falsche Betriebssystemversion gefunden. Es wird das Betriebssystem Windows 2000 benötigt.
1098	Die Installation von SafeGuard Easy ist fehlgeschlagen.
1099	Die Deinstallation von SafeGuard Easy ist fehlgeschlagen.

Allgemeine Fehler

1101	Selbstüberprüfung schlug fehl.
1102	Das Hilfesystem konnte nicht initialisiert werden.
1103	Eine Klasse konnte nicht registriert werden.
1104	Die Informationen über die Partitionskonfiguration sind inkonsistent.
1105	Ungültiger oder falscher Parameter definiert.
1106	Keiner oder zu wenige Parameter wurden definiert.
1107	Unbekannter Parameter definiert.
1108	Nicht genügend freier Speicher verfügbar.

1109	Modul '<Modulname>' konnte nicht geladen werden.
1110	Ein Dialog konnte nicht kreiert werden.
1111	Ein Dialog konnte nicht initialisiert werden.
1112	Ein Thread konnte nicht kreiert werden.
1113	Ein Fenster konnte nicht kreiert werden.
1114	Sie benötigen Administrator-Rechte, um zu installieren oder zu deinstallieren!
1115	Es ist eine Speicherschutzverletzung aufgetreten!
1117	Die Logdatei '<Dateiname>' konnte nicht geöffnet werden.
1118	Das Deinstallationsprogramm und das Administrationsprogramm von [PN] können nicht gleichzeitig gestartet sein.
1119	Kerneldatei nicht gefunden.
1120	Die Installation des 'control handler' schlug fehl.
1121	Unbekannte Umgebungsvariable definiert.
1122	Eine Umgebungsvariable konnte nicht gesetzt werden.
1123	Puffergröße unzureichend.
1124	Die DLL '%5' konnte nicht geladen werden!
1125	Die spezifizierte Funktion '%5' konnte nicht gefunden werden!
1126	Die Semaphore '%5' konnte nicht geöffnet werden!
1127	Das Modul '%5' konnte nicht freigegeben werden!
1128	Ein Ausnahmefehler trat auf während der Ausführung einer [PN] Subsystem Funktion! Last error code :%1Function return code: %2Module :%3Line number :%4Address :%5Bitte kontakten Sie: Utimaco Safeware AG!
1129	Ein kritischer Fehler trat auf bei der Ausführung einer oder mehrerer [PN] Subsystem Funktion(en)!Fatal error code: %1\nOS error code : %2\nModule : %3Function : %4\Beschreibung: [[MSGLINK]=%1].
1130	Belegter Hauptspeicher konnte nicht freigegeben werden.
1131	Eine Funktion wird zur Zeit nicht unterstützt.
1132	Zugriff verweigert.

1133 Programmstart von '<Name der Datei>' schlug fehl.

1134 Funktion oder Ressource nicht verfügbar.

1135 Der Prozess wurde vom Benutzer abgebrochen.

1136 Ungültiger oder falscher Eintrittspunkt definiert.

1137 Das System verändert zur Zeit einige Systemeinstellungen. Gegenwärtig sind keine weiteren Änderungen erlaubt.

1139 Ungültiger Datentyp für das Dialogfeld

1141 Kernel Backup schlug fehl.

1143 Definierte Arbeitsstation existiert nicht.

1144 Der Logon Klient 'SgeGina.dll' konnte nicht gefunden werden. Das limitiert ein Reihe von Funktionen von [PN] und kann ernsthafte Probleme nach sich ziehen, die einen Neuinstallation von [PN] oder des Betriebssystems erfordern könnten.

1145 Der Dienst 'SgeCtl.exe' konnte nicht gefunden werden. Das limitiert ein Reihe von Funktionen von [PN] und kann ernsthafte Probleme nach sich ziehen, die einen Neuinstallation von [PN] oder des Betriebssystems erfordern könnten.

1146 System Kernel ist defekt.

1147 Eine Partition wird gerade ver- oder entschlüsselt oder ein solcher Prozess wurde initiiert.\nEin Kernelbackup kann nur durchgeführt werden, wenn alle Ver-oder Entschlüsselungsprozesse beendet sind.

1148 Das Interface konnte nicht gefunden werden.
Klasse :%1 (%3)
Interface :%2
Result :%4 ([[OSERRLINK]=%5])\n\nMöglicherweise ist [[FILELINK]=SGE_INFO.DLL][[MSGLINK]=102] auf '%6' nicht installiert!

Fehler in der Konfigurationsdatei

1151 Die Konfigurationsdatei <Name der Datei> konnte nicht gefunden werden.

1152	Keine Konfigurationsdatei definiert.
1153	Sektionseintrag in der Konfigurationsdatei fehlt.
1154	Ungültiger Eintrag in der Konfigurationsdatei gefunden.
1155	Konfigurationsdatei <Name der Datei> konnte nicht gefunden werden.
1156	Fehler in Zeile <Name der Datei> der Konfigurationsdatei gefunden.
1158	Die angegebene Konfigurationsdatei konnte nicht gefunden werden!
1159	Ein unbekannter Befehl wurde in der Konfigurationsdatei gefunden.
1160	Unbekannter Typ einer Konfigurationsdatei gefunden.
1161	Typ der Konfigurationsdatei ist ungültig.
1162	Der Handle für die Konfigurationsdatei ist ungültig.
1163	Konfigurationsdatei für die Deinstallation konnte nicht erzeugt werden.
1164	Konfigurationsdatei zur Deinstallation konnte nicht erzeugt werden.
1165	Die Konfigurationsdatei <Name der Konfigurationsdatei> konnte nicht gefunden werden.
1166	Der Typ der Konfigurationsdatei ist ungültig.
1167	SGE1157: Ausführung der Konfigurationsdatei '<Name der Konfigurationsdatei>' schlug fehl.

MESSAGE Control Fehler

1171	Message ID <Nummer der ID> nicht gefunden.
1172	Kein Control Text für eine Control ID gefunden.
1173	Die Windows NT Logdatei konnte nicht geschrieben werden!

1174	Eine ungültige Datei oder ein ungültiger Message Link wurden gefunden: Message identifier: %1\nLink command : %2.
1175	Das Format der Messagedatei '<Name der Datei>' ist ungültig!
1176	Falsche Definition der Messagebox-Attribute

Passwortfehler

1181	Kein Systemverwalterpasswort definiert.
1182	Unbekanntes Passwort.
1183	Kein Passwort definiert.
1184	Definiertes Passwort ist zu kurz.
1185	Definiertes Passwort ist zu lang.
1186	Definierte Passworte stimmen nicht überein.
1187	Das Passwort ist trivial.\nWollen Sie ein anderes Passwort eingeben?
1188	Das vergebene Passwort existiert für einen anderen Benutzer. Wollen Sie das Passwort dennoch verwenden?
1189	Das vergebene Passwort enthält nicht die geforderte Anzahl von Buchstaben, Sonderbuchstaben, Ziffern und Symbolen.
1190	Das Passwort hat noch nicht sein definiertes Mindestalter erreicht.

Schlüsselfehler

1201	Kein Festplattenschlüssel angegeben.\n\nDie Festplattenverschlüsselung kann nur gesetzt werden, wenn ein Festplattenschlüssel angegeben wurde.
1202	Kein Diskettenschlüssel angegeben.\n\nDie Diskettenverschlüsselung kann nur gesetzt werden, wenn ein Diskettenschlüssel angegeben wurde.

1203	Kein Geräteschlüssel angegeben.\n\nDie Geräteverschlüsselung kann nur gesetzt werden, wenn ein Geräteschlüssel angegeben wurde.
1204	Der definierte Schlüssel ist zu lang.
1205	Der definierte Schlüssel ist zu kurz.
1206	Die angegebenen Schlüssel stimmen nicht überein.
1207	Kein Schlüssel definiert!
1208	Der Modus 'Bootschutz' verlangt einen Schlüssel für die Verschlüsselung der Festplatte!
1209	Der Modus 'Standard' verlangt einen Schlüssel für die Verschlüsselung der Festplatte!
1210	Der Schlüssel ist trivial.\nWollen Sie einen anderen Schlüssel angeben?

IPC Fehler

1221	IPC Server konnte nicht gestartet werden.
1222	IPC Client konnte nicht gestartet werden.
1223	IPC Verbindung konnte nicht aufgebaut werden.
1224	IPC Meldung konnte nicht aufgenommen werden.
1225	IPC Meldung konnte nicht abgesetzt werden.
1226	IPC Funktion IPC_SGE_PROCESS_DEF_MSG\nkonnte nicht verarbeitet werden.
1227	IPC Server konnte nicht geschlossen werden.
1228	IPC Klient konnte nicht geschlossen werden.
1229	IPC Thread konnte nicht gestartet werden.
1230	Das Warten auf eine IPC Meldung schlug fehl.
1231	IPC Kommunikationsobjekt nicht gefunden.

Laufwerksfehler

1241	Unbekanntes oder ungültiges Laufwerk definiert.
1242	Keine weiteren Laufwerke gefunden.
1243	Laufwerks-I/O-Operation schlug fehl.
1244	Lesezugriff von einem Laufwerk schlug fehl.
1245	Schreibzugriff auf ein Laufwerk schlug fehl.
1246	Startzugriff auf ein Laufwerk schlug fehl.
1247	Laufwerk nicht bereit!
1248	Sperren eines Laufwerks schlug fehl.
1249	Entsperren eines Laufwerks schlug fehl.
1250	Die Systemartition muss eine primäre Partition sein.\n\nDas ist z.B. notwendig, wenn die Option 'Unterstützung für Compaq Setup-Partition' aktiviert wurde.
1251	Freigeben eines Volumes schlug fehl.\n\nEventuell sind einige Dateien oder Fenster noch offen.
1252	Die erste physikalische Disk ist keine Festplatte.
1253	Alle Einträge in der Partitionstabelle des MBR Sectors auf der ersten Festplatte sind bereits belegt.\n\nDie Option „Unterstützung für Compaq Setup-Partition“ erfordert einen freien, unbenutzten Eintrag in der Partitionstabelle!
1254	System wurde im Kompatibilitätsmodus gestartet.
1255	Um SafeGuard Easy zu installieren, entfernen Sie bitte die steckbare Festplatte.
1256	Es sind keine Laufwerke dieses Typs vorhanden
1257	Interner Fehler beim Zugriff auf die Systempartition

SERVICE Fehler

1261	Informationen über ein Speicherobjekt für einen Systemdienst konnten nicht freigegeben werden.
1262	Fehler im Systemdienst-Dispatcher entdeckt.

1263 Systemdienst konnte nicht gestartet werden.

1264 Status des Systemdienstes konnte nicht gewechselt werden.

1265 Der Handler für den Systemdienst konnte nicht registriert werden.

1266 Die Funktion zur Dienste-Installation meldete einen Fehler!

1267 Der 'service information block' konnte nicht gefunden werden. Vermutlich ist nicht genügend Speicher verfügbar!\n\nErrorcode: %1.

REGISTRY Fehler

1271 Eintrag in der Registry konnte nicht geöffnet werden.

1272 Eintrag in der Registry konnte nicht gelesen werden.

1273 Eintrag in der Registry konnte nicht geschrieben werden.

1274 Eintrag in der Registry konnte nicht kreiert werden.

1275 Eintrag in der Registry konnte nicht gelöscht werden.

1276 Eintrag für einen Systemdienst in der Registry konnte nicht geöffnet werden.

1277 Eintrag für einen Systemdienst in der Registry konnte nicht kreiert werden.

1278 Eintrag für einen Systemdienst in der Registry konnte nicht gelöscht werden.

1279 Eintrag für einen Systemdienst in der Registry existiert bereits.

1280 Der 'Session Control Manager' konnte nicht geöffnet werden.

1281 Registryeintrag für eine Session konnte nicht gefunden werden.

1282 Ungültiger Registryeintrag entdeckt.

Datenbanktreiber-Fehler

1291 Keine weiteren Verschlüsselungstreiber gefunden.

1292	Datenbanktreiberdatei nicht gefunden.
1293	Fehler trat auf beim Lesen der Datenbanktreiberdatei.
1294	Datenbanktreiberdatei ist leer.
1295	Ungültiger oder illegaler Eintrag Eintrag in der Datenbanktreiberdatei.

CRAREA Fehler

1301	Zugriffsfehler auf das Installationslaufwerk.
1302	Anforderung nach Partitionsinformationen schlug fehl.
1303	Zugriff auf die Bootpartition schlug fehl.
1304	Ungültige Prozessoption definiert.
1305	Unbekanntes oder ungültiges Dateisystem defniert.
1306	Unterschied entdeckt zwischen dem aktuellen und dem definiertem Dateisystem.
1307	Unterschied entdeckt zwischen der aktuellen und der definierten Clustergröße.
1308	Ungültiger Start-Cluster für den Kernelbereich definiert.
1309	Ungültiger Start-Sektor für den Kernelbereich definiert.
1310	Ungültiger Partitionstyp definiert.
1311	Keine freien Cluster für den Kernel gefunden.
1312	Cluster konnten nicht als 'gebraucht' markiert werden.
1313	Cluster konnten nicht als 'gut' markiert werden.
1314	Cluster konnten nicht als 'unbenutzt' markiert werden.
1315	Cluster konnten nicht als 'schlecht' markiert werden.
1316	Cluster Informationen korrupt.
1317	Der als 'bad' markierte Bereich konnte nicht markiert werden.
1318	Ungültige Größe des Kernelbereichs definiert.
1319	Der MBR Sektor auf der ersten Festplatte konnte nicht ersetzt werden.

SGOCA Fehler

1401	Die angeforderten 'object communication area' Informationen existieren bereits.
1402	Die 'object communication area' existiert bereits.
1403	Die angeforderten 'object communication area' Informationen existieren bereits.
1404	Die 'object communication area' konnte nicht gefunden werden.
1405	Die angeforderte 'object communication area' Informationen existieren nicht.
1406	Zusätzliche 'object information data' gefunden.

SGUICL Fehler

1511	Die Komponenten Konfiguration konnte nicht geladen werden!

ADMLOGON Fehler

1601	Die Anmeldung war erfolglos. Versuchen Sie es bitte noch einmal !
1602	Das [PN] Subsystem erlaubt nicht mehr als 5 Anmeldeversuche. Sie müssen den Rechner neu starten und die Anwendung neu starten!
1603	Der Start der [PN] Logonkomponente schlug fehl.
1604	
1605	Der Logon an [PN] war erfolgreich, aber Sie haben nicht genügend Rechte, um das Produkt zu deinstallieren.

Administration Fehler - USER

1801	Der Benutzer '<Benutzername>' kann nicht erzeugt werden, weil die Maximalanzahl an Benutzern erreicht ist.

1802 Es ist nicht möglich, den Benutzer '*AUTOUSER' zu erzeugen oder zu löschen.

1803 Der Benutzer '<Benutzername>' existiert bereits. Bitte legen Sie den Benutzer unter einem anderen Namen an.

1804 Die Maximalanzahl an Benutzern wurde überschritten!

1805 Es ist nicht erlaubt, den Benutzer 'SYSTEM' anzulegen oder zu löschen. Nur ein Modifizieren ist erlaubt.

1806 Das Benutzerprofil erfordert einen Token für die Anmeldung an [[FILELINK]=SGE_INFO.DLL][[MSGLINK]=102].

1807 Die Applikation wartet bereits 30 sekunden auf Abschluß des Vorganges. Der Computer kann zu sehr beschäftigt sein. Sie können warten, bis der Vorgang beendet ist, oder möchten Sie abbrechen?

Migrationsassistent Fehler

2006 SGEInteg: Das Dateisystem ist inkonsistent. Die SafeGuard Easy-Migration schlug fehl. Bitte lesen Sie im SafeGuard Easy-Benutzerhandbuch nach, wie Sie den Fehler mittels SGEInteg /R reparieren können.

SGEGINA Fehler

2100 Der Auto Logon schlug fehl. Wollen Sie die Verbindung zwischen dem SafeGuard Easy Benutzer und dem Betriebssystem Benutzer editieren?

2101 Sie müssen ihr Passwort jetzt wechseln. \nDer Auto Logon (SAL) ist für diese Anmeldung deaktiviert!

Deinstallation Fehler

2201 Die Deinstallationsprozedur kann nicht gestartet werden, weil ein Chiffrier- oder Dechiffriervorgang gerade läuft!

2202 Die Deregistrierung einer Komponente ist fehlgeschlagen!

2203 Die Deinstallation von [[MSGFILE]=SGE_INFO.dll][[MSG-LINK=102] kann nicht fortgesetzt werden. Es wurde eine Festplatten gefunden, die vor der Installation nicht vorhanden war. Bitte entfernen Sie die nachträglich eingebaute Festplatte!

Erweiterte Installation - Fehler

2301 Das Installationspaket hat die falsche Version und kann nicht verwendet werden !

2302 Beim Installationsmodus 'Standard' oder 'Bootschutz' sind nicht mehr als 8 Partitionen pro Festplatte erlaubt!

2303 Eine COM Komponente konnte nicht registriert werden!

2304 Die Installation von [PN] benötigt den 'Windows Installer' von Microsoft. Nähere Informationen finden Sie im Handbuch oder in der README Datei.

2305 Falsche Betriebssystemversion vorgefunden. Das Betriebssystem Windows NT/2000 ist erforderlich!

Notfallassistent - Fehler

2401 Die Erzeugung der Kernelbackupdatei wurde abgebrochen!

2402 Nicht alle Notfalldateien konnten erfolgreich kopiert werden!

SAL Fehler

2501 Die SAL-Datei konnte nicht geöffnet werden

2502 Die SAL-Datei befindet sich in einem undefiniertem Zustand

2503 Undefinierter Fehler bei Dateioperationen

2504 SAL- Datei konnte nicht korrekt positioniert werden

2505 SAL-Datei Lesefehler

2506 SAL-Datei Schreibfehler

2507	Der angegebene Benutzer konnte nicht gefunden werden
2508	Keinen derzeitig angemeldeten Benutzer gefunden
2509	Es konnte nicht geschrieben werden, weil ein existierender Eintrag zu klein für den neuen Eintrag ist
2510	Der Zielpuffer ist zu klein für den ganzen Eintrag
2511	Kein Speicher verfügbar

Datenbanktreiber-Fehler

2601	Das Schreiben von Daten in die Datenbank schlug fehl !
2602	Das Lesen von Daten aus der Datenbank ist fehlgeschlagen !
2603	Die Erzeugung eines Eintrages in der Datenbank ist fehlgeschlagen !
2604	Das Löschen eines Eintrages aus der Datenbank ist fehlgeschlagen !
2605	Die Datenbank ist nicht erreichbar !

Interface Fehler

3001	Das COM Interface Object kann nicht verschlüsselt werden.\nInterface Name:%1\nFehler Nummer: %2Zusatzinformation:%3
3002	Die Ausführung einer Interface Methode ist fehlgeschlagen. Folgende detailierte Fehler Informationen wurden gemeldet: \nFehler Nummer: %1\nhResult: %2\nBeschreibung: %3\nInterface :%4\nBitte kontaktieren Sie Ihren Systemadministrator!

Client/Server Fehler

3201	Der Server oder der Client ist gegenwärtig beschäftigt und kann die Anforderung jetzt nicht bearbeiten.

Administrationskonsole-Fehler

3301	Datenbankverbindung fehlgeschlagen!
3302	Serverkonsole-Schnittstelle nicht gefunden!
3303	Fernadministration-Schnittstelle nicht gefunden!
3304	Dateikonfigurationsassistent-Schnittstelle nicht gefunden!